Trend Micro InterScan Messaging Security Suite™

安心を、ひとつ上のステージへ。

TREND MICRO™

インストールガイド

トレンドマイクロへのお客様情報の送信について

「フィッシング詐欺対策」「URL フィルタ」では、Webサイトが安全かどうかの判定のために、お客さまがアクセスしたURLの情報を暗号化してトレンドマイクロのサーバに送信します。

サーバに送信されたURL情報は、Webサイトの安全性の確認、および本機能の改良の目的にのみ利用されます。

また、これらの機能を有効にしたうえで、コモンゲートウェイインタフェースアプリケーションを使用しているサーバで構築されているWebサイトにアクセスし、ID、パスワード等を入力した場合には、お客様がアクセスしたWebページのURLにお客様が入力したID、パスワード等が含まれた状態でトレンドマイクロのサーバに送信される場合があります。この場合、トレンドマイクロでは、お客様がアクセスするWebページの安全性の確認のため、これらのお客様より受領した情報にもとづき、お客様がアクセスするWebページのセキュリティチェックを実施します。

「ソフトウェア安全性評価サービス」では、プログラムが安全かどうかの判定のために、プログラムの情報をトレンドマイクロのサーバに送信します。
「ウイルストラッキング/TrendCareプログラム」では、検出されたウイルス/脅威名、検出数、国/地域、感染元となったWebサイトのURLを、統計を取るためにトレンドマイクロのサーバに送信します。
「迷惑メール対策ツール」では、弊社製品の改良目的および迷惑メールの撲滅のため、トレンドマイクロのサーバに該当メールを送信します。また、迷惑メールの削減、迷惑メールによる被害の抑制を目指している政府関係機関に対して迷惑メール本体を開示する場合があります。

輸出規制について

本製品は、外国為替及び外国貿易法、U.S. Export Administration Regulations、およびその他の国における輸出規制品目に該当している場合があります。したがって、本製品が輸出規制品目に該当する場合、適正な政府の許可なくして、禁輸国もしくは貿易制裁国の企業、居住者、国民、または、取引禁止者、取引禁止企業に対して、輸出もしくは再輸出できません。このような規制についての情報は以下のウェブサイトから見つけることができます。

「http://www.treas.gov/ofac/」、および「http://www.bis.doc.gov/complianceandenforcement/ListsToCheck.htm」

2008年12月現在、米国により定められる禁輸国は、キューバ、イラン、北朝鮮、スーダン、シリアが含まれています。

あなたは本製品に関連した米国輸出管理法令の違法行為に対して責任があります。本契約の同意により、あなたは、あなたが米国により現時点で禁止されている国の居住者もしくは国民ではないこと、別途本製品を受け取ることが禁止されていないことを確認します。また、大量破壊を目的とした、核兵器、化学兵器、生物兵器、ミサイルの開発、設計、製造、生産を行うために使用しないことに同意します。

複数年契約について

お客様が複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。
複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。各製品のサポート提供期間は以下のウェブサイトからご確認いただけます。

http://jp.trendmicro.com/jp/support/lifecycle/index.html

著作権について

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。トレンドマイクロ株式会社が事前に承諾している場合を除き、形態および手段を問わず、本書またはその一部を複製することは禁じられています。本ドキュメントの作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとします。本書およびその記述内容は予告なしに変更される場合があります。

TRENDMICRO、ウイルスバスター、ウイルスバスター On-Line-Scan、PC-cillin、InterScan、INTERSCAN VIRUSWALL、ISVW、InterScanWebManager、ISWM、InterScan Message Security Suite、InterScan Web Security Suite、IWSS、TRENDMICRO SERVERPROTECT、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Micro Policy Server、トレンドマイクロ・プレミアム・サポート・プログラム、License for Enterprise Information Security、LEISec、Trend Park、Trend Labs、Trend Micro Enterprise Protection Strategy、InterScan Gateway Security Appliance、Trend Micro Network VirusWall、Network VirusWall Enforcer、Trend Flex Security、EPS、Trend Micro EPS、LEAKPROOF、Trendプロテクト、Expert on Guard、InterScan Messaging Security Appliance、InterScan Web Security Appliance、InterScan Messaging Hosted Security、およびDataDNAは、トレンドマイクロ株式会社の登録商標です。

本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。

Copyright © 2008-2009 Trend Micro Incorporated. All rights reserved.

P/N: IMSSFF-AE0104_R2 (2009/01)

目次

はじめに 9

ドキュメント 10

対象読者 11

ドキュメントの表記規則 11

第 1 章　製品の概要 13

InterScan MSS 7.0 について 14

新機能 14

InterScan MSS の主な特長と利点 16

スパイウェアと他の種類のグレーウェア 24

Trend Micro Control Manager について 25

Trend Micro Control Manager との統合 26

第 2 章　システム要件とコンポーネント 31

システム要件 32

InterScan MSS コンポーネントについて 35

InterScan MSS 管理データベース 35

セントラルコントローラ 35

検索サービス 36

ポリシーサービス 37

ポリシーの同期 37

エンドユーザメール隔離サービス 38

プライマリおよびセカンダリエンドユーザメール隔離サービス 38
エンドユーザメール隔離サーバコンポーネント 38
Apache および mod_jk 39
Tomcat 39
Struts フレームワーク 40
エンドユーザメール隔離アプリケーション 40
エンドユーザメール隔離データベース 41
IP フィルタ 41
Trend Micro Network Reputation Services 42
Trend Micro Network Reputation Services の種類 42
IP プロファイラの機能 43
Trend Micro Network Reputation Service の機能 43

第 3 章 配置計画 45

配置チェックリスト 46
コンポーネントおよびサブモジュールのインストール 49
InterScan MSS で使用されるポート 52
ネットワークトポロジの検討 55
ファイアウォールなしのインストール 55
ファイアウォールの外側へのインストール 56
受信トラフィック 56
送信トラフィック 56
ファイアウォールの内側へのインストール 57
受信トラフィック 57
送信トラフィック 58
既存の SMTP ゲートウェイ上へのインストール 59
受信トラフィック 60
送信トラフィック 60

DMZ 内へのインストール 60
受信トラフィック 61
送信トラフィック 61
インストールシナリオについて 61
集中インストール 62
複数の検索サービスのインストール 64
複数の検索サービスとポリシーサービスのインストール 64
複数のエンドユーザメール隔離サービスのインストール 66
エンドユーザメール隔離を配置する際のその他の検討事項 68
サーバ間の通信 69
複雑な分散インストール 69
WAN へのインストール 72
Trend Micro Control Manager 72
WAN での配置構成におけるフォールトトレランスとフェイルオーバー 74
IP フィルタ 75
IP フィルタ機能を付加した InterScan MSS の配置 75
フェイルオーバーについて 76

第 4 章 インストールとアップグレード 79

集中インストール 80
検索サービスとエンドユーザメール隔離サービス / データベースの複数インストール 92
以前にインストールされたコンポーネントが存在しない場合のコンポーネントの追加 92
以前にインストールされたコンポーネントが存在する場合のコンポーネントの追加 101
複雑な分散インストール 104
サイレントインストール 105
インストール手順の記録 106

サイレントインストールスクリプトの実行 107
InterScan MSS 5.18 からのアップグレード 108
アップグレード前のバックアップ 108
移行の実行 109
移行されない設定 112
アップグレード後のロールバック 113
アンインストールの実行 114
サイレントアンインストール 118
MSDE から SQL Server 2005 Express へのアップグレード 119
SQL Server 2005 Express のインストールの前提条件 119
インストールされた MSDE から SQL Server 2005 Express へのアップグレード 119
手順 1 — すべての InterScan MSS サービスの停止 120
手順 2 — InterScan MSS データベースのバックアップの作成 120
手順 3 — SQL Server 2005 Express のインストール 121
手順 4 — データベース管理者のパスワードのリセット 122
手順 5 — InterScan MSS サービスの開始 123
新規インストール時の SQL Server 2005 Express との統合 124
手順 1 — SQL Server 2005 Express のインストール 124
手順 2 — ネットワークアクセスの有効化 125
手順 3 — SQL Server Browser サービスのスタートアップの自動化 125
手順 4 — InterScan MSS 7.0 のインストール 125

第 5 章 トラブルシューティングとサポート情報 127

トラブルシューティング 128
よくある質問 (Q&A) 129
インストール 129
アップグレード 132

製品サポート情報 136
サポートサービスについて 136
製品 Q&A のご案内 137
セキュリティ情報 137
セキュリティ情報の入手先 137
トレンドマイクロへのウイルス解析依頼 138
ウイルス解析サポートセンター「TrendLabs」 139

索引 141

はじめに

Trend Micro InterScan Messaging Security Suite 7.0 インストールガイドをお読みいただきありがとうございます。本書では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の機能、システム要件、およびインストールとアップグレードの方法について説明しています。

InterScan MSS の設定方法については「Trend Micro InterScan Messaging Security Suite 7.0 管理者ガイド」を、またユーザインタフェースの詳細については管理コンソールからオンラインヘルプを参照してください。

この章の内容は、次のとおりです。

- 10 ページの「ドキュメント」
- 11 ページの「対象読者」
- 11 ページの「ドキュメントの表記規則」

ドキュメント

InterScan MSS 7.0 には、次のドキュメントが付属しています。

- **インストールガイド** — InterScan MSS の機能、システム要件、およびさまざまなネットワーク環境における InterScan MSS の配置およびアップグレード方法について説明しています。
- **管理者ガイド** — InterScan MSS のインストールと実行、およびインストール後の設定と管理方法について説明しています。
- **オンラインヘルプ** — 各フィールドの詳細や、ユーザインタフェースを使用したあらゆる機能の設定方法について説明しています。オンラインヘルプにアクセスするには、管理コンソールを開いて、ヘルプアイコン ( ) をクリックしてください。
- Readme **ファイル** — 他のドキュメントに記載されていない可能性のある最新の製品情報を提供します。トピックには、機能の説明、インストールのヒント、既知の問題、および製品のリリースの履歴などが含まれます。

インストールガイド、管理者ガイドおよび Readme ファイルは、
http://www.trendmicro.co.jp/download/ から入手できます。

対象読者

InterScan MSS のドキュメントは、中規模から大規模企業の IT 管理者を対象に書かれています。本書は、読者の方に、次の知識を含め、メールメッセージングネットワークの専門的な知識があることを前提としています。

- SMTP および POP3 プロトコル
- Microsoft Exchange などの Message Transfer Agent (MTA)
- LDAP
- データベース管理

本書は、読者の方に、ウイルス対策やスパムメール対策のテクノロジに関する知識があることを前提としていません。

ドキュメントの表記規則

情報を簡単に検索し、理解できるように、InterScan MSS のドキュメントでは、次の表記規則を使用しています。

表記	説明
注意 :	設定上の注意
ヒント :	推奨事項
警告 :	避けるべき操作や設定についての注意

第 1 章

製品の概要

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の特長、機能、およびテクノロジについて説明します。また、既存のスパムメール対策機能を強化することのできる他のトレンドマイクロ製品の基本情報も示します。

この章の内容は次のとおりです。

- 14 ページの「InterScan MSS 7.0 について」
- 14 ページの「新機能」
- 16 ページの「InterScan MSS の主な特長と利点」
- 24 ページの「スパイウェアと他の種類のグレーウェア」
- 25 ページの「Trend Micro Control Manager について」

InterScan MSS 7.0 について

InterScan MSS 7.0 では、メールを完全に保護するために、ウイルス対策、スパムメール対策、フィッシング対策、およびコンテンツフィルタの機能が一元化されています。この柔軟性の高いソフトウェアソリューションには、高い評価を受けているウイルス対策機能およびゼロデイ攻撃対策機能が備わっており、既知のウイルスおよび変種 / 亜種のウイルスをブロックします。

InterScan MSS のスパムメール対策は、Trend Micro Network Reputation Services (以下、NRS) の第 1 防御レベルに、IP プロファイラによるカスタマイズ可能なトラフィック管理機能とさまざまな技術を取り入れた強力な複合エンジンを組み合わせた多層構造になっています。多言語スパムメール対策では、グローバルな企業に対して追加サポートが提供されます。高度なコンテンツフィルタにより、各種規格との適合および企業管理が達成され、機密情報が保護されます。InterScan MSS の保護機能により、単一でスケーラビリティの高いプラットフォームで、一元化管理が容易になり、ゲートウェイにおける総合的なメールセキュリティが実現します。

新機能

表 1-1 に、バージョン 7.0 の新機能の概要を示します。

新機能	説明
さまざまなウイルス対策および不正プログラムのポリシー	さまざまな InterScan MSS ポリシーと LDAP のサポートにより、さまざまな条件に基づいて、特定の送信者および受信者に適用するフィルタを設定できます。
ログおよびレポート機能の一元化	一元管理される詳細なレポート機能により、ポリシーに一致した送受信者の上位を示す統計データや、トラフィックデータを作成できます。 ログ機能も一元化されているため、管理者はメッセージに関連する活動をすばやく監査できます。

表 1-1.　新機能

新機能	説明
アーカイブおよび隔離領域管理の一元化	InterScan MSS の複数のメッセージ隔離領域とアーカイブ領域を簡単に検索できます。
スケーラブルなエンドユーザメール隔離	複数のエンドユーザメール隔離サービスが、スパムメールとして検出、隔離されたメールメッセージの表示機能を提供します。 InterScan MSS でエンドユーザメール隔離の通知機能を使用することで、ヘルプデスクの管理作業にかかるコストを低減できます。
さまざまなスパムメール対策テクノロジ	次の 3 層にわたるスパムメール対策が用意されています。 ・接続層でスパムメール送信者をフィルタする NRS ・高度なプロファイル (SMTP IDS) を使用してメールサーバを攻撃から保護する IP プロファイラ ・スパムメールを的確に検出し、削除するスパムメール検索エンジン
IntelliTrap	IntelliTrap は、さまざまな圧縮スキームで圧縮されたウイルスがメールを通じてネットワークに侵入するリスクを軽減できるよう、圧縮ファイルのヒューリスティック評価機能を提供します。
管理タスクの委任	LDAP が統合されたアカウント管理により、ユーザは設定タスクごとに管理権限を割り当てることができます。
設定ウィザードによる簡単配置	InterScan MSS をすぐに起動して実行できるように、使いやすい設定ウィザードが用意されています。
高度な MTA 機能	TLS や、ドメインベースの配信などの MTA 機能により、InterScan MSS は安全な方法で効果的にメールを処理します。
移行	アップグレード手順が簡単なため、セットアップ時は最小限の操作で設定内容を移行できます。
メールの監査とトラッキング	すべてのメッセージが詳細にログされるため、メッセージフローに関する問題を追跡して特定できます。

表 1-1. 新機能

新機能	説明
Trend Micro Control Manager (以下、Control Manager) との統合	さまざまな対応機能に加え、Control Manager からログクエリを実行します。26 ページの「Trend Micro Control Manager との統合」を参照してください。
8 ビットから 7 ビットへの MIME 変換のサポート	InterScan MSS 7.0 Service Pack 1 は、RFC 1652「8 ビット MIME 転送のための SMTP サービス拡張」で定義されている規格に基づく、8 ビットから 7 ビットへの MIME 変換に対応しています。SMTP サーバの次のホップが 8 ビット MIME に対応していない場合、8 ビット MIME メッセージは 7 ビット MIME メッセージに変換されます。

表 1-1. 新機能

InterScan MSS の主な特長と利点

特長	説明	利点
ウイルス対策	InterScan MSS は、トレンドマイクロの検索エンジンとパターンマッチングと呼ばれるテクノロジを使用して、ウイルスを検出します。検索エンジンは、ゲートウェイを介して受信したファイルに含まれるコードを、パターンファイルに格納されている既知のウイルスのバイナリパターンと比較します。パターンの一致を検出すると、検索エンジンはポリシールールの設定に応じて、そのウイルスコードの削除、メッセージの隔離などの処理を実行することによりファイル内のウイルス駆除を試みます。	InterScan MSS では、ウイルス検索およびコンテンツ検索機能が強化されているため、メッセージングシステムの動作効率を最適な状態で維持できます。

表 1-2. 主な特長と利点

特長	説明	利点
IntelliTrap	ウイルス作成者は通常、さまざまなファイル圧縮スキームを使用してウイルスフィルタを回避しようとします。IntelliTrap は、これらの圧縮ファイルのヒューリスティック評価機能を提供します。 場合により、脅威ではないファイルにセキュリティ上のリスクがあると誤って識別される可能性もあるため、IntelliTrap を有効にするときは、このカテゴリに分類された添付ファイルを隔離することをお勧めします。また、ユーザが日常的に圧縮ファイルをやり取りしている場合は、この機能を無効にした方がよい場合もあります。 初期設定では、IntelliTrap はウイルス対策ポリシーで検索条件の 1 つとして有効になっており、セキュリティ上のリスクとして誤って分類された添付ファイルは隔離されるように設定されています。	さまざまなファイル圧縮スキームで圧縮されたウイルスがメールを通じてネットワークに侵入するリスクを軽減できるようにします。
コンテンツ管理	InterScan MSS は、ネットワーク経由で送受信されるメールのメッセージと添付ファイルを解析し、適切な内容かどうかをチェックします。	個人的なメールのやり取りや巨大な添付ファイルなど、企業が不適切と見なす内容は、InterScan MSS を使用して効果的にブロックしたり、受信を遅延したりできます。
その他のメール脅威からの保護		
DoS 攻撃	巨大な添付ファイルでメールサーバをオーバーフローさせたり、複数のウイルスや多重圧縮ファイルが含まれるメッセージを送信したりすることで、悪意のあるユーザがメール処理を妨害することがあります。	InterScan MSS を使用すると、どのような特性を持つメッセージを SMTP ゲートウェイで阻止するかを設定できるため、DoS 攻撃のリスクを低減できます。

表 1-2.　主な特長と利点

特長	説明	利点
不正な メールコンテンツ	実行可能プログラムや、マクロが埋め込まれたドキュメントなど、ウイルスはさまざまな種類の添付ファイルに潜んでいる可能性があります。HTML スクリプトファイル、HTML リンク、Java アプレット、ActiveX コントロールが含まれるメッセージも、有害な処理を実行する可能性があります。	InterScan MSS では、SMTP ゲートウェイの通過を許可するメッセージの種類を設定できます。
生産性の劣化	ビジネスに関係のないメールトラフィックは、多くの企業で問題となっています。スパムメールメッセージはネットワーク帯域幅を消費し、従業員の生産性に影響します。従業員の中には、会社のメッセージングシステムから個人的なメッセージを送信したり、巨大なマルチメディアファイルを転送したり、業務時間内に個人的なビジネスを行ったりする人もいます。	ほとんどの企業では、メッセージングシステムの使用許容範囲を示すポリシーを制定しています。InterScan MSS は、企業の既存のポリシーを強化し、確実に準拠させることのできるツールを提供します。
法的責任と ビジネスの信頼性	メールが不正に使用されると、企業の法的責任が問われる場合があります。従業員が性的または人種的嫌がらせを行っていたり、他の違法活動に携わっていたりするかもしれません。また、従業員の不正行為により、社内のメッセージングシステムから機密情報が漏えいする可能性もあります。企業のメールサーバから不適切なメッセージが配信されれば、そのメッセージの内容が企業の持論と異なるものであったとしても、企業の評判を損ねることになります。	InterScan MSS には、コンテンツを監視してブロックするツールが装備されているため、不適切な内容や機密事項が含まれるメッセージがゲートウェイを通過するリスクを低減できます。

表 1-2.　主な特長と利点

特長	説明	利点
マスメーリング型ウイルスの抑制	企業のメッセージングシステムを介して偽造メッセージを自動的に広めるメール送信型ウイルスは、クリーンナップに費用がかかり、ユーザ間にパニックを引き起こす可能性があります。 InterScan MSS では、マスメーリング型ウイルスを検出したときに、他の種類のウイルスとは異なる処置を講じます。 たとえば、重要な情報が含まれる Microsoft Office ドキュメントにマクロウイルスが検出された場合、重要な情報が失われないように、メッセージ全体を削除する代わりにメッセージを隔離するようプログラムを設定できます。また一方で、マスメーリング型ウイルスが検出されたときに、プログラムでメッセージ全体を自動的に削除することも可能です。	マスメーリング型ウイルスが含まれたメッセージを自動的に削除すると、復元の価値がないメッセージやファイルの検索、隔離などにサーバリソースを消費しないようにできます。 既知のマスメーリング型ウイルスの識別情報は、マスメーリング型パターンファイルに含まれています。このパターンは、TrendLabs (トレンドラボ) のアップデートサーバを使用してアップデートされます。これらの種類のウイルスとそのメールコンテナを自動的に削除するように指定すれば、リソースが節約されると共に、従業員からのヘルプデスクへの問い合わせや、大規模感染後のクリーンナップ作業から解放されます。

表 1-2.　主な特長と利点

特長	説明	利点
スパイウェアと他の種類のグレーウェア		
スパイウェアと他の種類のグレーウェア	クライアントは、ウイルス以外のスパイウェア、アドウェア、ダイヤラーなどの潜在的な脅威のリスクにもさらされています。詳細については、24 ページの「スパイウェアと他の種類のグレーウェア」を参照してください。	InterScan MSS が持つ、スパイウェアやその他の種類のグレーウェアからの保護機能により、セキュリティの上でも、機密性に関しても、法的な面でも、企業のリスクが大幅に軽減されます。
総合的なスパムメール対策		
スパムメール対策 (コンテンツ検索)	InterScan MSS では、オプションでスパムメール対策 (コンテンツ検索) 機能をインストールすることもできます。この機能を使用するには、別途アクティベーションコードが必要になります。詳細については、販売店にお問い合わせください。 InterScan MSS のスパムメール対策機能は、組み込みのスパムメールフィルタを使用して機能します。このフィルタは、スパムメール対策用のアクティベーションコードを入力してアクティベーションを完了した時点で有効になります。 **注意** : InterScan MSS のスパムメール対策機能は、IP プロファイラと NRS を設定する前にアクティベートしてください。	InterScan MSS のスパムメール対策機能では、最新のコンテンツ処理および統計分析に基づく検出テクノロジが使用されています。コンテンツ分析機能を採用したことで、パフォーマンスの高いリアルタイムの検出が可能となっています。スパムメールの送信者が手法を変更した場合でも、容易に対応できます。

表 1-2. 主な特長と利点

特長	説明	利点
IP プロファイラと NRS によるスパムメールフィルタ	IP プロファイラは、自己学習能力と十分なカスタマイズ性を備えており、スパムメールや他の潜在的な脅威を送信するコンピュータの IP アドレスを未然にブロックします。NRS は、トレンドマイクロの中央データベースで管理される既知のスパムメール送信者の IP アドレスをブロックします。 詳細については、以下を参照してください。 ・41 ページの「IP フィルタ」 ・42 ページの「Trend Micro Network Reputation Services」 ・43 ページの「IP プロファイラの機能」 ・43 ページの「Trend Micro Network Reputation Service の機能」	IP プロファイラおよび NRS から成る IP フィルタ機能を統合することで、InterScan MSS は IP レベルでスパムメール送信者をブロックできます。
その他		
LDAP およびドメインベースのポリシー	Lotus Domino、Microsoft Active Directory などの LDAP ディレクトリサービスをユーザグループの定義および管理者権限に使用している場合、LDAP を設定できます。 Web 隔離ツールを使用するには、LDAP を有効にする必要があります。	LDAP を使用すると、さまざまなルールを定義して、企業のメールの使用ガイドラインを適用することができます。送信者および受信者のアドレスに基づいて、個人またはグループ用のルールを定義できます。
Web ベースの管理コンソール	Web ベースの管理コンソールを使用すると、InterScan MSS のポリシーや設定を、Web 上で必要に応じて設定できます。	Web ベースのコンソールは、SSL に準拠しているので、高い安全性が確保されます。

表 1-2.　主な特長と利点

特長	説明	利点
エンドユーザ メール隔離	InterScan MSS には、スパムメール管理を強化するための Web ベースのエンドユーザメール隔離が用意されています。Web ベースのエンドユーザメール隔離を使用すると、エンドユーザは各自のスパムメールの処理方法を管理できます。InterScan MSS のスパムメール対策機能によって、スパムメールが隔離されます。これらのメッセージは、エンドユーザメール隔離によってデータベース内でインデックスが付けられます。それにより、エンドユーザはメッセージを再確認して、削除したり配信を許可したりできるようになります。	Web ベースのエンドユーザメール隔離コンソールを使用して、エンドユーザは InterScan MSS によって隔離されるメッセージを管理できます。
管理タスクの委任	InterScan MSS には、管理コンソールにさまざまなアクセス権限を作成する機能が用意されています。管理者のログオンアカウントごとに、アクセスを許可する管理コンソールのセクションを選択できます。	別々の従業員に管理役割を委任して、人材のバックアップ体制を構築し、管理業務全般の共有を促進できます。
一元化された レポート機能	一元化されたレポート機能では、必要に応じてそのつどレポートを作成することも、指定されたときにレポートを作成することも可能です。	InterScan MSS の稼動状況を解析できます。 必要なときにそのつどレポートを作成する場合、レポート内容の種類を必要に応じて指定できます。また、日次、週次、および月次ベースで自動生成するように InterScan MSS を設定することもできます。
システムの可用性 の監視	組み込みエージェントが InterScan MSS サーバの状態を監視し、メールフローを妨害する可能性のある違反状況が発生した場合に、メールまたは SNMP トラップを通じて通知を配信します。	システム障害の検出をメールで通知するので、ただちに適切な処置を講じて、ダウンタイムを最小限にすることができます。

表 1-2.　主な特長と利点

特長	説明	利点
POP3 メール検索	管理コンソールから、POP3 メール検索を有効または無効にできます。	SMTP トラフィックのほかに、InterScan MSS では、ネットワーク内のメッセージングクライアントがメッセージを受信する際に、ゲートウェイで POP3 メッセージも検索できます。
クラスタアーキテクチャ	本バージョンの InterScan MSS は、分散配置が可能になるように設計されています。	さまざまな InterScan MSS コンポーネントを個別のコンピュータにインストールすることも、いくつかの同じコンポーネントを複数のコンピュータにインストールすることもできます。たとえば、メッセージングのボリュームに応じて、InterScan MSS の追加の検索サービスコンポーネントを別のサーバにインストールし、すべてのサーバで同じポリシーサービスを使用することができます。
Control Manager との統合	Control Manager は、ウイルス対策プログラムとコンテンツセキュリティプログラムを、その物理的な位置やプラットフォームに関係なく中央から制御できるようにするソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルスおよびコンテンツセキュリティポリシーの管理を簡略化します。 詳細については、25 ページの「Trend Micro Control Manager について」を参照してください。	Control Manage を通して提供される大規模感染予防サービスにより、大規模感染のリスクを低減できます。新種のメール送信型ウイルスが検出されると、トレンドラボから詳細なコンテンツフィルタを使用するポリシーが発行されるため、InterScan MSS では、メッセージ内の疑わしい特性を識別して、メッセージをブロックすることができます。これらのルールは、最新のパターンファイルが提供されるまでの期間、感染の機会を最小限に抑えるのに役立ちます。

表 1-2.　主な特長と利点

スパイウェアと他の種類のグレーウェア

クライアントは、ウイルス以外の脅威のリスクにもさらされています。グレーウェアは、ネットワーク上のコンピュータのパフォーマンスに悪影響を与え、セキュリティの上でも、機密性に関しても、法的な面でも、企業に深刻なリスクをもたらします (表 1-3 を参照)。

スパイウェア / グレーウェアの種類	説明
スパイウェア / グレーウェア	アカウントユーザ名やパスワードなどのデータを収集し、サードパーティに送信します。
アドウェア	広告を表示したり、Web ブラウザを通じてそのユーザをさまざまな広告のターゲットとするために、ユーザの Web サーフィンの好みなどのデータを収集したりします。
ダイヤラー	コンピュータのインターネット設定を変更し、あらかじめ設定された電話番号に、コンピュータがモデムを通じて自動的にダイヤルするようにします。
ジョークプログラム	CD-ROM トレイを開閉したり、大量のメッセージボックスを表示したりするなど、コンピュータの異常動作を引き起こします。
ハッキングツール	ハッカーがコンピュータに侵入するために使用するツールです。
リモートアクセスツール	ハッカーがコンピュータをリモートにアクセスして制御するためのツールです。
パスワード解読アプリケーション	ハッカーがアカウントユーザ名とパスワードを解読するためのツールです。
その他	上記以外の種類。

表 1-3. スパイウェア / グレーウェアの種類

Trend Micro Control Manager について

Control Manager は、ウイルス対策プログラムとコンテンツセキュリティプログラムを、その物理的な位置やプラットフォームに関係なく中央から制御できるようにするソフトウェア管理ソリューションです。このアプリケーションは、企業のウイルスおよびコンテンツセキュリティポリシーの管理を簡略化します。

Control Manager は、次のコンポーネントで構成されます。

- **Control Manager サーバ** — Control Manager サーバは、Control Manager アプリケーションがインストールされるコンピュータです。Control Manager の Web ベースの管理コンソールは、このサーバに生成されます。

  注意： InterScan MSS 7.0 Windows を Control Manager で管理する場合、Control Manager Server 3.5 Patch 3 以降をインストールする必要があります。

- **エージェント** — エージェントは、Control Manager が製品を管理できるように、製品サーバ上にインストールされるアプリケーションです。エージェントは Control Manager サーバからコマンドを受信して、管理対象製品に適用します。また、製品からログを収集して、Control Manager に送信します。

  注意： エージェントは個別にインストールする必要はありません。InterScan MSS をインストールすると、自動的にインストールされます。

- **エンティティ** — エンティティは、Control Manager の製品ディレクトリ上の管理製品を表します。エンティティセクションのディレクトリツリーには、各エンティティがアイコンで表示されます。ディレクトリツリーは、Control Manager に登録されたすべての管理下のエンティティの組織図です。InterScan MSS は、Control Manager 管理コンソールの 1 つのエンティティといえます。

  検索サービスをインストールする際に、Control Manager エージェントも自動的にインストールされます。エージェントが有効になると、検索サービスはそれぞれ Control Manager サーバに登録され、個別のエンティティとして表示されます。

注意： Control Manager を使用して InterScan MSS を管理する場合は、Control Manager サーバのバージョン 3.5 以降を使用します。Control Manager の詳細およびアップデートプログラムについては、トレンドマイクロの最新版ダウンロードサイトを参照してください。
http://www.trendmicro.co.jp/download/product.asp?productid=7

Trend Micro Control Manager との統合

表 1-4 は、InterScan MSS でサポートされている Control Manager の機能を示しています。

機能	説明	サポートの有無
双方向の通信	双方向の通信では、InterScan MSS または Control Manager のどちらからでも通信処理を開始できます。	サポートなし Control Manager との通信処理を開始できるのは、InterScan MSS のみです。
大規模感染予防ポリシー	大規模感染予防ポリシーは、トレンドラボで開発された、大規模感染に素早く対応するポリシーです。これには、InterScan MSS サーバやクライアントが感染する可能性を低減するために InterScan MSS で実行される、一連の処理が含まれています。 トレンドマイクロアップデートサーバは、Control Manager を通してこのポリシーを InterScan MSS に配置します。	サポートあり
クエリに対するログのアップロード	InterScan MSS ウイルスログ、コンテンツセキュリティログ、NRS ログを、クエリの目的で Control Manager にアップロードします。	サポートあり

表 1-4.　サポートされている Control Manager の機能

機能	説明	サポートの有無
シングルサインオン	InterScan MSS Web 管理コンソールにログオンせずに、Control Manager から InterScan MSS を直接管理します。	サポートなし Control Manager から InterScan MSS を管理するには、まず、InterScan MSS Web 管理コンソールにログオンする必要があります。
設定の複製	Control Manager から、既存の InterScan MSS サーバの設定を新しい InterScan MSS サーバへ複製します。	サポートあり
パターンファイルのアップデート	Control Manager から、ウイルス / 不正プログラムのパターンファイルをアップデートします。	サポートあり
検索エンジンのアップデート	Control Manager から検索エンジンをアップデートします。	サポートあり
製品コンポーネントのアップデート	Control Manager から、Patch や HotFix などの InterScan MSS 製品コンポーネントをアップデートします。	サポートなし 製品コンポーネントのアップデートの方法については、特定の Patch または HotFix の Readme ファイルを参照してください。

表 1-4.　サポートされている Control Manager の機能

機能	説明	サポートの有無
ユーザインタフェースリダイレクトによる設定	Control Manager 内からアクセスできる InterScan MSS Web 管理コンソールを使用して、InterScan MSS を設定します。	サポートあり
製品登録の更新	Control Manager から InterScan MSS 製品ライセンスを更新します。	サポートあり
Control Manager 上のメール関連のレポート	Control Manager から次の InterScan MSS メール関連のレポートを生成します。 ・上位 10 位のウイルス検出ポイント ・すべてのエンティティのウイルス感染リスト ・上位 10 位の感染メール送信者のレポート ・上位 10 位のセキュリティ違反のレポート ・ウイルス感染チャネル - 製品の関係レポート ・頻度別のイベントのフィルタ処理 ・ポリシー別のイベントのフィルタ処理 ・ゲートウェイメッセージングスパムメールの概要レポート ・ゲートウェイメッセージングスパムメールの概要レポート (ドメイン用)	サポートあり

表 1-4.　サポートされている Control Manager の機能

機能	説明	サポートの有無
Control Manager エージェントのインストール / アンインストール	Control Manager から、InterScan MSS Control Manager エージェントをインストール / アンインストールします。	サポートなし InterScan MSS Control Manager エージェントは、InterScan MSS をインストールした時点で自動的にインストールされます。エージェントを有効 / 無効にするには、InterScan MSS Web 管理コンソールから次の操作を実行します。 1. メニューから [管理]→ [接続] を選択します。 2. [Control Manager サーバ] タブをクリックします。 3. エージェントを有効 / 無効にするには、[Control Manager エージェントを有効にする] の横のチェックボックスを、それぞれオン / オフにします。
イベント通知	Control Manager から InterScan MSS イベント通知を送信します。	サポートあり
すべてのコマンドに対するコマンド追跡	Control Manager から InterScan MSS に発行されるコマンドのステータスを追跡します。	サポートあり

表 1-4.　サポートされている Control Manager の機能

第 2 章

システム要件とコンポーネント

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) を管理するために必要な要件と、InterScan MSS が機能する上で必要な各種のソフトウェアコンポーネントについて説明します。

この章の内容は次のとおりです。

- 32 ページの「システム要件」
- 35 ページの「InterScan MSS コンポーネントについて」

システム要件

表 2-1 に、InterScan MSS を実行する上で推奨されるシステムの最小要件を示します。

OS	・Microsoft Windows Server 2003 SP1、SP2 Edition ・Microsoft Windows Server 2003 R2、SP2 Edition ・Microsoft Windows Server 2003 x64 SP2 Edition ・Microsoft Windows Server 2003 x64 R2、SP2 Edition ・Microsoft Windows 2000 Server SP4 ・Microsoft Windows 2000 Advanced Server SP4 **注意** : Microsoft Windows 2000 SP4 では、InterScan MSS データベース接続用に Microsoft MDAC 2.8 SP1 以上が必要です。MDAC の最新バージョンは、次の Microsoft サイトからダウンロードできます。 http://www.microsoft.com/downloads/details.aspx?FamilyID=78cac895-efc2-4f8e-a9e0-3a1afbd5922e&DisplayLang=ja
推奨 CPU	デュアル構成の Pentium 4 3GHz 以上
最小 CPU	Intel Pentium 4 2.4GHz
推奨メモリ	2GB の RAM
最小メモリ	1GB の RAM
推奨ハードディスク領域	・メール保存用に 10GB ・管理データベース用に 50GB 以上 ・エンドユーザメール隔離データベース用に 20GB 以上 ・作業隔離フォルダ用に 40GB 以上 **注意** : これらの要件は、1 日あたり 500,000 件のメールメッセージ、50% の隔離率で、1ヵ月あたりに保存されるログ数に基づいています。

表 2-1.　システム要件

最小ハードディスク領域	・メール保存用に 5GB
推奨スワップ領域	スワップ領域は、4GB から物理メモリの 4 倍のサイズの範囲で設定することをお勧めします。 **注意** : 各 InterScan MSS の下位プロセスには、120MB のメモリを消費します。したがって、パフォーマンスをよくするには、ピーク時のトラフィックを処理できるだけの十分な物理メモリおよび仮想メモリを割り当てる必要があります。 たとえば、2GB の物理メモリと 8GB のスワップ領域を持つコンピュータでは 75 件の下位プロセスを作成できます。必要なスワップ領域は、他のアプリケーションのメモリ消費量に応じて異なります。InterScan MSS は、アップストリーム MTA からの 75 件の接続要求を同時に処理できます。
ブラウザ	・Internet Explorer 6 SP1/SP2 または Internet Explorer 7 ・Firefox 1.5
Microsoft SQL Server	・Microsoft SQL Server Desktop Edition (MSDE) SP4 ・Microsoft SQL Server 2005 SP1、SP2 ・Microsoft SQL Server 2000 SP4 ・Microsoft SQL Server 2005 Express SP1、SP2 **注意** : MSDE 2000 には次の制限が適用されます。 - データ量 2GB - 同時ユーザ接続または作業負荷数 5 1 日のメールトラフィックが 30,000 件を上回る場合や、InterScan MSS エンドユーザメール隔離を使用している場合、MSDE を使用しないようにしてください。これは、レポートとログクエリ結果の保存用に十分な空き領域を確保する必要があるためです。 また、MSDE のメインストリームサポートは、2008 年 4 月 8 日に終了します。MSDE から、4GB までデータを処理できる SQL Server 2005 Express にアップグレードすることをお勧めします。119 ページの「MSDE から SQL Server 2005 Express へのアップグレード」を参照してください。
Microsoft Data Access Components	Microsoft Data Access Components (MDAC) 2.8 SP1 以上

表 2-1. システム要件

LDAP サーバ	・Microsoft Active Directory 2000 または 2003 ・IBM Lotus Domino 6.0 以上 ・Sun One LDAP 5.2 以上

表 2-1.　システム要件

注意： MSDE を使用して InterScan MSS 管理データベースとエンドユーザメール隔離データベースをインストールした場合、これらのデータベースは初期設定で C:¥Program Files¥Trend Micro¥MSDE に配置されます。SQL Server を使用している場合、管理データベースとエンドユーザメール隔離データベースは、SQL Server のデータフォルダに配置されます。InterScan MSS 隔離作業フォルダは、初期設定で C:¥Program Files¥Trend Micro¥IMSS¥queue¥ に配置されます。

注意： システム要件に記載されているオペレーティングシステムの種類やハードディスク容量などは、本ドキュメント作成時点の情報です。システム要件は、オペレーティングシステムのサポート終了や、弊社製品の改良、検索エンジンやパターンファイルのバージョンアップなどに伴い、変更、追加、または削除される場合があります。また、製品の運用環境によっては、ログファイルの保存、他のソフトウェアとの共存などにより、必要となるメモリサイズやハードディスク容量も異なりますので、ご注意ください。最新のシステム要件については、弊社 Web サイトやサポート窓口にご確認ください。

InterScan MSS コンポーネントについて

InterScan MSS の新しいアーキテクチャでは、メッセージ処理で実行されるタスクごとに、この製品を個別のコンポーネントに分類しています。以下の項では、各コンポーネントの概要を示します。

InterScan MSS のコンポーネントは、単一のコンピュータまはた複数のコンピュータにインストールできます。コンポーネントの連携の仕組みについては、61 ページの「インストールシナリオについて」の図解を参照してください。

InterScan MSS 管理データベース

InterScan MSS 管理データベースには、グローバル設定情報がすべて保存されます。データベースには、サーバ設定、ポリシー情報、ログ情報、およびコンポーネント間で共有されるその他のデータが保持されます。InterScan MSS をインストールする際は、他のコンポーネントをインストールする前に、データベースサーバをインストールして、データベーステーブルを作成するための適切なクエリを実行する必要があります。バンドルされている Microsoft SQL Server Desktop Engine (MSDE) データベースをインストールするか、または既存の Microsoft SQL Server を使用できます。

セントラルコントローラ

セントラルコントローラには、Web サーバコンポーネントが含まれ、このコンポーネントにより、管理者が InterScan MSS を設定および制御するための管理コンソールを Web ブラウザで表示できるようになります。この管理コンソールは、各種のコンポーネントによって検索やログなどのメッセージ処理タスクの実行に使用される InterScan MSS データベースと管理者間のインタフェースとして機能します。

検索サービス

検索サービスとして設定されたサーバでは、次の操作が実行されます。

- SMTP および POP3 メッセージングトラフィックの受け入れ
- ポリシーサービスからのポリシーの要求
- 適用可能なポリシーに基づいたメッセージの評価
- 評価結果に基づいたメッセージへの適切な処理
- 隔離されたメッセージとアーカイブされたメッセージのローカルでの保存
- ポリシーとシステムの動作のローカルログへの記録、および指定された間隔での InterScan MSS データベースのログの一部の自動更新。その際、隔離されたアイテムとログを検索できるよう、インデックスが作成されます。

検索サービスの設定は、管理コンソールを使用して検索サービスすべてにグローバルに適用されるため、同じハードウェア構成のサーバを指定して、検索サービスとして機能させます。同じハードウェア構成のコンピュータが環境内にない場合は、最小限のリソースで検索サービスを保護できるよう、検索サービスの上限を設定する必要があります。たとえば、2 つの検索サービスがあり、1 つのハードディスクが 10GB、もう 1 つのハードディスクが 80GB の場合は、ディスク使用量の上限を 9GB に設定して、最小限のリソースでコンピュータを保護する必要があります。

別の方法として、検索サービスのローカルの設定ファイルを編集し、上限値をローカルに設定することもできます。設定ファイルに設定した上限値は、グローバル設定より優先されます。一度ローカルに設定された検索サービスは、管理コンソールからは設定できなくなります。また、インタフェースに一部のローカル設定の詳細が反映されない場合があります。

注意： .ini ファイルを変更してカスタマイズする際は、注意が必要です。必要に応じて、サポート担当者にお問い合わせください。

ポリシーサービス

パフォーマンスを高め、ルールの検索を効率的に実行するために、InterScan MSS はポリシーサービスのメモリ内キャッシュを使用して、メッセージングルールを格納します。ポリシーサービスは、ルールをキャッシュに格納することで、検索サービスに対するルールのリモートストアとして機能します。これにより、データベースを検索する必要もなくなり、関連するネットワークやディスク I/O のオーバーヘッドも排除できます。また、このメカニズムによって検索サービスの効率もアップするため、ほとんどのメッセージ検索タスクを、ディスクを使用せずに検索サービスのメモリで実行することができます。

ポリシーの同期

InterScan MSS 管理データベースのスキーマには、バージョニングメカニズムが含まれています。ポリシーサービスは、データベースのバージョンを定期的にチェックします。データベース内のバージョン番号が、ポリシーサービスにキャッシュされているバージョンと異なる場合、ポリシーサービスはデータベースクエリを実行して最新のバージョンを取得します。これにより、キャッシュ内のデータベースのバージョンとデータベースとの同期がとれ、データベース全体に対して新規のエントリまたは変更されたエントリをチェックする必要がなくなります。

InterScan MSS の管理コンソールから変更を行うと、その変更はポリシーサービスに即時に反映されます。

エンドユーザメール隔離サービス

プライマリのエンドユーザメール隔離サービスには InterScan MSS の管理コンソールと同様の Web ベースコンソールが生成されるため、ユーザは、処理されたスパムメールの表示、削除、または再送を行うことができます。

プライマリおよびセカンダリエンドユーザメール隔離サービス

負荷分散を支援するために、追加のエンドユーザメール隔離サービスをインストールすることができます。これを「セカンダリサービス」と呼びます。インストールした 1 台目のエンドユーザメール隔離サービスは、「プライマリサービス」と呼ばれ、Apache を実行してセカンダリサービスと連動します。

エンドユーザメール隔離サーバコンポーネント

エンドユーザメール隔離サーバには、次のソフトウェアコンポーネントが含まれています。

- Apache HTTP **サーバ** — エンドユーザからの HTTPS 要求を受け入れ、それぞれの要求をインストールされているすべてのエンドユーザメール隔離サービスに分散させます。Apache は、プライマリエンドユーザメール隔離サーバにのみインストールされています。
- Tomcat Application **サーバ** — エンドユーザから HTTPS 要求を受け入れ、要求を Struts に渡します。
- Struts **フレームワーク** — エンドユーザに対するページ表示のフローを制御します。
- **エンドユーザメール隔離アプリケーション** — 他の InterScan MSS コンポーネントと通信して、エンドユーザメール隔離コンソールのロジックを実装します。

Tomcat および Apache ソフトウェアは {IMSS}¥UI ディレクトリにインストールされます。他のコンポーネントは {IMSS}¥UI¥euqUI ディレクトリにインストールされます。

Apache と Tomcat はどちらも、Windows の [管理ツール] メニューにある [サービス] 管理コンソール (services.msc) によって制御されます。

Apache および mod_jk

Apache HTTP サーバのバージョン 2.0.58 (http://httpd.apache.org/ を参照) は、プライマリエンドユーザメール隔離サーバにインストールされ、Apache Tomcat Connector mod_jk (http://tomcat.apache.org/connectors-doc/ を参照) ロードブルモジュールを使用して、すべての要求をローカルでインストールされた Tomcat Application サーバへ転送します。

Apache は、標準の Apache ServerRoot 構造を持つ、{IMSS}¥UI¥apache ディレクトリにインストールされます。Apache のメイン設定ファイル ({IMSS}¥UI¥euqUI¥conf ディレクトリ内の EUQ.conf) では、Apache によって転送される要求をすべて受信する Tomcat スレッドの名前と共に、Apache の受信接続の TCP ポート (8447)、サービス接続の最大数 (150) および mod_jk の設定が定義されています。

Tomcat

エンドユーザメール隔離サーバでは、Tomcat Application サーバを使用してエンドユーザからの要求が処理されます。また、プライマリエンドユーザメール隔離サーバにインストールされた Tomcat Application サーバも、Apache HTTP サーバからの要求を受け入れ、Apache JServ Protocol バージョン 1.3 プロトコル AJP13 (http://tomcat.apache.org/tomcat-3.3-doc/AJPv13.html を参照) とラウンドロビンアルゴリズムを使用して、インストールされているすべてのエンドユーザメール隔離サーバに負荷を分散させます。

Tomcat 設定ファイル ({IMSS}¥UI¥euqUI¥conf ディレクトリ内の server.xml) では、TCP ポート (8446)、プロトコル (HTTPS)、SSL キーリングの場所 ({IMSS}¥UI¥tomcat¥sslkey¥.keystore) など、さまざまな設定が定義されています。

{IMSS}¥UI¥euqUI¥conf ディレクトリ内の workers.properties 設定ファイル (http://tomcat.apache.org/tomcat-3.3-doc/Tomcat-Workers-HowTo.html) に、Tomcat worker スレッドの設定が記述されています。ここでは、loadbalancer と worker の 2 種類のスレッドが定義されています。loadbalancer スレッドは、インストールされているすべてのエンドユーザメール隔離サーバに負荷を分散させます。worker スレッドは、受信要求を処理し、エンドユーザメール隔離アプリケーションを実行します。この設定ファイルは Manager により自動的に管理され、tb_component_list データベーステーブルから使用できるすべてのエンドユーザメール隔離サーバに関する情報に基づいて再起動時に更新されます。

AJP13 プロトコルにより、Apache と Tomcat 間は常時接続され、この接続を使用して、オーバヘッドを増やさずに要求を Tomcat へ転送し、その要求の処理結果を受信します。

Struts フレームワーク

Struts は Model-View-Controller Java ベースのフレームワークであり、Struts の使用によって HTTP 要求を処理する複雑な Java ベースのアプリケーションの開発と制御が容易になります (http://struts.apache.org/ を参照)。

つまり、Struts は受信 HTTP 要求、その要求を処理する Java プログラム (Servlet) およびこの処理の結果を表示するために使用される Java Server Page (JSP) の間の関係を制御します。

Struts 自体は、struts-config-common.xml および struts-config-enduser.xml という設定ファイルによって設定された struts.jar アーカイブファイル内でパッケージ化された一連の Java クラスです。

エンドユーザメール隔離アプリケーション

エンドユーザメール隔離アプリケーションは Java で記述され、エンドユーザの要求に基づいて、隔離されたメールメッセージを表示、隔離解除、または削除します。また、エンドユーザが承認済み送信者リストを管理できるようにします。

この機能を実装するために、エンドユーザメール隔離アプリケーションはデータベースにアクセスしてマネージャと通信します。

エンドユーザメール隔離アプリケーションは、{IMSS}¥UI¥euqUI¥ROOT¥WEB-INF¥classes ディレクトリ内に格納された com.trendmicro.imss.ui パッケージの一連の Java クラスと {IMSS}¥UI¥euqUI¥ROOT¥jsp ディレクトリ内に格納された一連の Java Server Pages として実装されます。

エンドユーザメール隔離アプリケーションは、{IMSS}¥log¥imssuieuq.< **日付** >.< **カウント** > ログファイルにログエントリを書き込みます。imss.ini ファイルの [general]¥ log_level 管理設定は、エンドユーザメール隔離アプリケーションによって書き込まれる情報量を制御します。ログに記録される情報量を増やすには、log_level を「デバッグ」に設定し、services.msc を使用して Tomcat を再起動します。

エンドユーザメール隔離データベース

エンドユーザメール隔離データベースには、隔離されたスパムメールの情報、およびエンドユーザの承認済み送信者リストが格納されます。エンドユーザメール隔離サービスをインストールする場合は、エンドユーザメール隔離データベース (スケーラビリティを高める場合は複数のデータベース) もインストールする必要があります。また、既存の SQL Server を使用して、エンドユーザメール隔離データベースをインストールすることもできます。

次のいずれかのオプションで、imsseuq と呼ばれるエンドユーザメール隔離データベースをインストールできます。

- 管理データベースをホストするデータベースサーバにインストール
- ネットワーク内で使用可能な別のデータベースにインストール
- データベースサーバのソフトウェアと共にインストール

1 つの InterScan MSS インスタンスは、最大 8 つのエンドユーザメール隔離データベースに対応できます。エンドユーザメール隔離データは、すべてのエンドユーザメール隔離データベースに分散されます。あるデータベースが消失した場合、このデータベースに格納されたデータを持つユーザは隔離されたデータにアクセスできなくなります。

IP フィルタ

InterScan MSS には、オプションの IP フィルタも搭載されています。これは、次の 2 つの機能で構成されます。

- **IP プロファイラ** — IP プロファイラを使用すると、メールトラフィックの解析に使用するしきい値を設定できます。ある IP アドレスから送信されたトラフィックがこの設定に違反している場合、IP プロファイラはその送信者の IP アドレスを自身のデータベースに追加して、同じ IP アドレスからの接続要求をブロックします。

IP プロファイラは、次の 4 つの潜在的なインターネット脅威をすべて検出します。

- **スパムメール** — 不要な広告的な内容が含まれるメール。
- **ウイルス** — トロイの木馬などの各種のウイルス脅威。
- **ディレクトリハーベスト攻撃** (DHA) — 有効なドメイン名を持つ任意のメール名を組み合わせ、任意のメールアドレスを作成して有効なメールアドレスを収集するために、スパムメール発信者が使用する方法。生成されたこれらのメールアドレスにメールが送信されます。メールメッセージが配信されると、そのメールアドレスは実在するアドレスと見なされ、スパムメールデータベースに追加されます。
- **バウンスメール** — メールサーバを使用して、差出人フィールドにターゲットのメールドメインを挿入したメールメッセージを生成する攻撃。生成されたメールメッセージは偽アドレスに送信された後、ターゲットのメールサーバに戻されます。これにより、メールサーバを氾濫させます。

- NRS — 既知のスパムメール送信者からのメールを IP レベルでブロックします。

Trend Micro Network Reputation Services

NRS は、接続要求のあったインターネットプロトコル (IP) アドレスを Trend Micro Threat Protection Network にルーティングして、大規模な評価データベースで検証することで、スパムメールがコンピュータネットワークに侵入する前に検出してブロックするように設計されています。

Trend Micro Network Reputation Services の種類

NRS では、次の 2 種類のサービスが用意されています。

- Trend Micro RBL+ Service — 総合的で信頼できる評価データベースで IP アドレスを検証することによって、スパムメールを送信元に基づいてブロックします。指定したメールサーバによって、不明ホストからのメールメッセージの受信時に常に RBL+ データベースに対して DNS クエリが実行されます。そのホストが RBL+ データベースにリストされている場合、接続を拒否してその送信者からのスパムメールをブロックできます。

- Trend Micro Network Anti-Spam Service — スパムメールの送信元で膨大なメッセージの送信処理が行われている最中に、その送信元を特定し、メッセージの送信を停止させる、リアルタイムの動的ソリューションです。Trend Micro Network Anti-Spam Service は、RBL+ サービス同様、DNS クエリベースのサービスです。このサービスの中心になるのが、RBL+ データベースと、動的リアルタイムデータベースである QIL データベースです。この 2 つのデータベースはそれぞれ異なるエントリを持ち、IP アドレスの重複はありません。これらのデータベースによって、ゾンビや BGP 攻撃、およびその他のきわめて動的なスパムメール送信元に素早く対応できる、効率の高いデータベースが確保されます。

IP プロファイラの機能

IP プロファイラは、潜在的な脅威を含むメールを送信するコンピュータの IP アドレスを事前に学習します。InterScan MSS でいつ IP アドレスに指定の処理を開始するかは、いくつかの条件をカスタマイズすることで指定できます。条件は潜在的な脅威に応じて異なりますが、InterScan MSS が IP アドレスとしきい値を監視する期間はいずれも共通です。

次のプロセスは、InterScan MSS が送信側メールサーバから接続要求を受信した後に実行されます。

1. MTA から IP プロファイラの DNS サーバにクエリが送信され、IP アドレスがブロックリストに含まれているかどうかが確認されます。
2. IP アドレスがブロックリストに含まれている場合、接続要求は拒否されます。IP アドレスがブロックリストに含まれていない場合、IP プロファイラに指定されたしきい値の条件に従って、InterScan MSS でメールトラフィックが解析されます。
3. メールトラフィックが条件に違反している場合、InterScan MSS はその送信者の IP アドレスをブロックリストに追加します。

Trend Micro Network Reputation Service の機能

NRS は、ドメインネームサーバ (DNS) のクエリベースのサービスです。次のプロセスは、InterScan MSS が送信側メールサーバから接続要求を受信した後に実行されます。

1. InterScan MSS が、接続を要求しているコンピュータの IP アドレスを記録します。
2. InterScan MSS が、その IP アドレスを NRS の DNS サーバに転送し、評価データベースに問い合わせを行います。IP アドレスが既にスパムメールとして報告されている場合、そのアドレスは問い合わせの時点で既にデータベースに存在しています。
3. レコードが存在している場合、NRS は InterScan MSS に永続的または一時的に接続要求をブロックするよう指示します。要求をブロックするかどうかは、スパムメールのソースの種類、履歴、現在の活動レベル、およびその他の観察パラメータによって決まります。

図 2-1. は、NRS の機能を図示したものです。

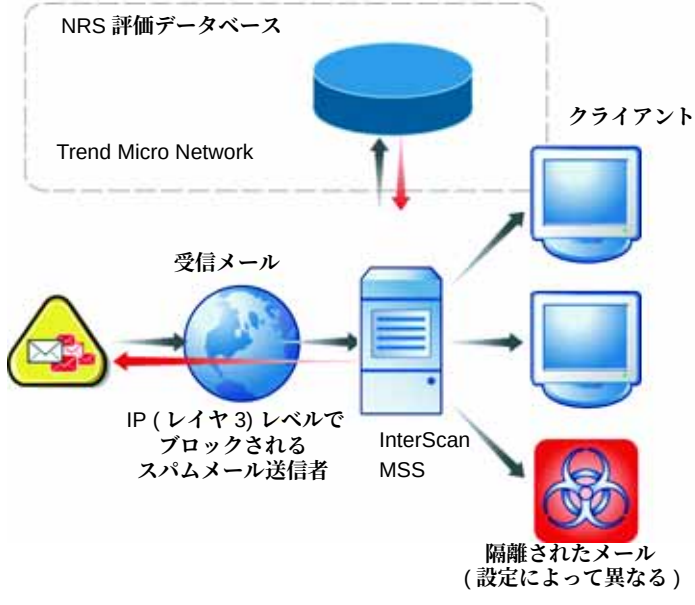


図 2-1. NRS の機能

NRS の処理の詳細については、次のサイトを参照してください。

http://jp.trendmicro.com/jp/products/enterprise/ers/ersa/index.html

第 3 章

配置計画

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の配置計画の手順について説明します。

この章の内容は次のとおりです。

- 46 ページの「配置チェックリスト」
- 49 ページの「コンポーネントおよびサブモジュールのインストール」
- 52 ページの「InterScan MSS で使用されるポート」
- 55 ページの「ネットワークトポロジの検討」
- 61 ページの「インストールシナリオについて」
- 75 ページの「IP フィルタ」
- 76 ページの「フェイルオーバーについて」

配置チェックリスト

配置チェックリストでは、InterScan MSS 配置のためのインストールの前後のタスクに関する手順を段階的に示します。

チェックマーク (完了時)	タスク	オプション	参照
	手順 1 — InterScan MSS の場所の特定		
	InterScan MSS をインストールするネットワーク上の場所を次のいずれかから選択します。		
	・ファイアウォールなし		55 ページの「ファイアウォールなしのインストール」
	・ファイアウォールの外側		56 ページの「ファイアウォールの外側へのインストール」
	・ファイアウォールの内側		57 ページの「ファイアウォールの内側へのインストール」
	・既存の SMTP ゲートウェイ上		59 ページの「既存の SMTP ゲートウェイ上へのインストール」
	・DMZ 内		60 ページの「DMZ 内へのインストール」
	手順 2 — 範囲の計画		
	InterScan MSS をインストールするのは、単一のサーバか複数のサーバかを選択します。		
	・集中インストール		62 ページの「集中インストール」
	・複数の検索サービス		64 ページの「複数の検索サービスのインストール」

チェックマーク (完了時)	タスク	オプション	参照
	・複数のエンドユーザメール隔離		66 ページの「複数のエンドユーザメール隔離サービスのインストール」
	・複雑な分散インストール		69 ページの「複雑な分散インストール」
	・広域ネットワーク		72 ページの「WAN へのインストール」
	注意 : フェイルオーバーの方法を検討してから、範囲を決定することをお勧めします。		76 ページの「フェイルオーバーについて」
	手順 3 — インストールまたはアップグレード		
	InterScan MSS の新規インストールまたは前バージョンからのアップグレードを実行します。		
	・InterScan MSS コンポーネントのインストール		80 ページの「集中インストール」
	・前バージョンからのアップグレード		108ページの「InterScan MSS 5.18 からのアップグレード」
	手順 4 — InterScan MSS の基本設定		
	設定ウィザードに従って、セントラルコントローラの設定を手順 8 まで進めます。		
	設定ウィザードを使用した設定		管理者ガイドの「設定ウィザードでの基本設定の実行」の項
	手順 5 — サービスの開始		
	さまざまな脅威からネットワークを保護する InterScan MSS サービスを起動します。		
	・検索サービス		管理者ガイドの「InterScan MSS サービス」の項
	・ポリシー		
	・エンドユーザメール隔離	サポートあり	

チェックマーク (完了時)	タスク	オプション	参照
	手順 6 — InterScan MSS のその他の設定		
	InterScan MSS のさまざまな設定を行い、InterScan MSS を起動します。		
	・IP フィルタのルール	サポートあり	管理者ガイドの「IP フィルタサービス」の項
	・SMTP ルーティング		管理者ガイドの「SMTP メッセージの検索」の項
	・POP3 設定	サポートあり	管理者ガイドの「POP3 メッセージの検索」の項
	・ポリシーおよび検索の除外		管理者ガイドの「ポリシーの管理」の項
	・コンポーネントの手動アップデートの実行と予約アップデートの設定		管理者ガイドの「検索エンジンとパターンファイルのアップデート」の項
	・ログの設定		管理者ガイドの「ログの設定」の項
	手順 7 — InterScan MSS のバックアップ		
	システム障害時の予防措置として、InterScan MSS 管理データベースのバックアップを作成します。		
	InterScan MSS 管理データベースのバックアップ		管理者ガイドの「InterScan MSS のバックアップ」の項

コンポーネントおよびサブモジュールのインストール

InterScan MSS コンポーネントをインストールすると、追加のサブモジュールも自動的にインストールされます。表 3-1 は各コンポーネントのサブモジュールを示しています。

メインコンポーネント	インストールされるサブモジュール	サブモジュールの説明
InterScan MSS 管理データベース	管理データベース	すべてのグローバルな設定が保存されたメインの InterScan MSS 管理データベース。
	データベースサーバ *	InterScan MSS 管理データベースを実行するサーバ。
セントラルコントローラ	Apache Tomcat	InterScan MSS 管理コンソール用の Web サーバで、これを使用して設定を行います。
	Named Server*	IP プロファイラの DNS サーバ。
	FoxDNS	IP プロファイラ用の IP アドレスのブロックリストおよび許可リストが含まれており、そのリストを DNS サーバに書き込みます。
	IMSSMGR	InterScan MSS 関連のプロセスを管理するモジュール。

表 3-1. コンポーネントおよびサブモジュールのインストール

メインコンポーネント	インストールされるサブモジュール	サブモジュールの説明
検索サービス	検索サービス	すべてのメール検索処理を実行します。
	ポリシーサービス	検索サービスに対するルールのリモートストアです。ルールがキャッシュに格納されるため、データベースを検索する必要がなくなります。
	Control Manager エージェント	Trend Micro Control Manager (以下、Control Manager) が InterScan MSS を管理するのに必要なソフトウェアコンポーネント。
	IMSSMGR	検索サービスの処理を管理するモジュール。
	SMTP サービス	Trend Micro MTA/MDA
	IP プロファイラ	Trend Micro MTA の一部
	Trend Micro Network Reputation Services (以下、NRS)	Trend Micro MTA の一部
エンドユーザメール隔離サービス	Apache Tomcat	エンドユーザメール隔離管理コンソールの Web サーバです。これによって、ユーザはスパムメールとして InterScan MSS が隔離したメールメッセージにアクセスできます。
	Apache サービス	複数のエンドユーザメール隔離サービスのインストールを選択した場合に、負荷分散のためにプライマリエンドユーザメール隔離サービスと共にこのモジュールをインストールします。
	IMSSMGR	エンドユーザメール隔離の処理を管理するモジュール。

表 3-1. コンポーネントおよびサブモジュールのインストール

メインコンポーネント	インストールされるサブモジュール	サブモジュールの説明
エンドユーザメール隔離データベース	エンドユーザメール隔離データベース	InterScan MSS がスパムメールとして隔離したすべてのメールメッセージを含むデータベース。
	データベースサーバ *	エンドユーザメール隔離データベースを実行するサーバ。
アスタリスク (*) の付いたサブモジュールは、メインコンポーネントをインストールする際に、必要に応じてインストールを選択できるサブコンポーネントです。		

表 3-1. コンポーネントおよびサブモジュールのインストール

InterScan MSS で使用されるポート

InterScan MSS で使用されるポートについては、表 3-2 を参照してください。

ポート番号	コンポーネントと役割	設定の保存先
25	MTA サービスポート。 メールサーバは、このポートで待機してメッセージを受信します。ファイアウォールでは、このポートを開放する必要があります。開放されていないと、メールを受信できません。	管理コンソールのメニューから、[管理]→[InterScan MSS の設定]→[SMTP ルーティング]→[接続] の順に選択します。
110	InterScan MSS 検索サービス用の一般 POP3 ポート。検索サービスはこのポートを使用して、POP3 要求を受け入れ、すべての POP3 サーバに対して POP3 メールを検索します。	管理コンソールのメニューから、[管理]→[InterScan MSS の設定]→[接続]→[POP3] の順に選択します。
5060	ポリシーサーバ待機ポート。検索サービスはメッセージごとにこのポートに接続して、一致するルールがないかどうか問い合わせます。	管理コンソールのメニューから、[管理]→[InterScan MSS の設定]→[接続]→[コンポーネント] の順に選択します。
8005	Tomcat 管理コマンドを処理する Admin UI Web サーバ (Tomcat) 管理ポート。	{IMSS}¥UI¥adminUI¥conf¥server.xml: Server¥port
8009	エンドユーザメール隔離コンソール Tomcat AJP ポート。このポートを使用して、複数の Tomcat サーバと Apache HTTP サーバ間の負荷分散を実行します。	{IMSS}¥UI¥euqUI¥conf¥server.xml: Server¥Service¥Connector (protocol=AJP¥1.3)¥port
8015	Tomcat 管理コマンドを処理する Tomcat 管理ポート。	{IMSS}¥UI¥euqUI¥conf¥server.xml: Server¥port

表 3-2.　InterScan MSS ポート

ポート番号	コンポーネントと役割	設定の保存先
8445	Admin UI 待機ポート。Web ブラウザを使用して管理コンソールにログオンするには、このポートを開放する必要があります。	Tomcat listen port: {IMSS}¥UI¥adminUI¥conf¥server.xml: Server¥Service¥Connector¥port
8446	エンドユーザメール隔離サービス待機ポート。	{IMSS}¥UI¥euqUI¥conf¥server.xml: Server¥Service¥Connector¥port
8447	負荷分散したエンドユーザメール隔離の待機ポート。	{IMSS}¥UI¥euqUI¥conf¥EUQ.conf: Listen¥VirtualHost¥ServerName
10024	InterScan MSS 検索サービスの再処理ポート。管理データベースの中央隔離領域やエンドユーザメール隔離データベースから隔離解除されたメッセージは、このポートに送信され再処理されます。	imss.ini¥[Socket_3]¥proxy_port
10026	InterScan MSS によって生成された通知メッセージの配信など、内部使用向けの InterScan MSS「パススルー」SMTP ポート。 このポートに送信されたすべてのメッセージは、InterScan MSS によって検索されません。セキュリティを考慮しているため、このポートがバインドされているのは InterScan MSS サーバのループバックインタフェース (127.0.0.1) のみです。そのため、他のコンピュータからはアクセスできません。ファイアウォールでは、このポートを開放する必要がありません。	tsmtpd.ini

表 3-2.　InterScan MSS ポート

ポート番号	コンポーネントと役割	設定の保存先
15505	InterScan MSS マネージャの待機ポート。InterScan MSS マネージャは、このポートを使用して管理コンソールからの管理コマンド (サービスの起動 / 停止など) を受け入れます。また、隔離 / アーカイブのクエリ結果も、このポートを使用して管理コンソールおよびエンドユーザメール隔離管理コンソールに送信されます。	管理コンソールのメニューから、[管理]→[InterScan MSS の設定]→[接続]→[コンポーネント] の順に選択します。
関連するサービスが有効にされている場合、InterScan MSS によって次のポートが使用されます。		
389	LDAP サーバ待機ポート。	管理コンソールのメニューから、[管理]→[InterScan MSS の設定]→[接続]→[LDAP] の順に選択します。
80	Microsoft IIS http 待機ポート。Control Manager サーバが Microsoft IIS に依存している場合、Control Manager を使用して InterScan MSS を管理する際に、このポートが必要になります。	管理コンソールのメニューから、[管理]→[InterScan MSSの設定]→[接続]→[Control Manager サーバ] の順に選択します。
443	Microsoft IIS https 待機ポート。Control Manager サーバが Microsoft IIS に依存している場合、Control Manager を使用して InterScan MSS を管理する際に、このポートが必要になります。	管理コンソールのメニューから、[管理]→[InterScan MSSの設定]→[接続]→[Control Manager サーバ] の順に選択します。
88	Kerberos レルム用 KDC ポート。	InterScan MSS サーバからは設定できません。
53	Bind サービス待機ポート。このポートを変更しないでください。	InterScan MSS サーバからは設定できません。

表 3-2. InterScan MSS ポート

ネットワークトポロジの検討

SMTP ゲートウェイで既存のメッセージング環境に InterScan MSS を配置します。この項では、さまざまなネットワークトポロジにおける InterScan MSS の配置場所を構成ごとに図解付きで示すと共に、他のゲートウェイサービスの一般的な設定手順について説明します。

注意： 以下の図では、InterScan MSS を集中インストールする場合を想定しています。インストールされた InterScan MSS は、それぞれ個別の論理単位として機能するため、これらのトポロジは分散配置インストールにも同様に適用されます。ただし、InterScan MSS では検索サービス間でメッセージが分散されないため、サードパーティ製のソフトウェアまたはスイッチを使用して、InterScan MSS 検索コンポーネントの複数のインスタンス間でトラフィックを分散する必要があります。

ファイアウォールなしのインストール

図 3-1. は、ネットワークにファイアウォールが設定されていない場合の InterScan MSS の配置方法を示しています。

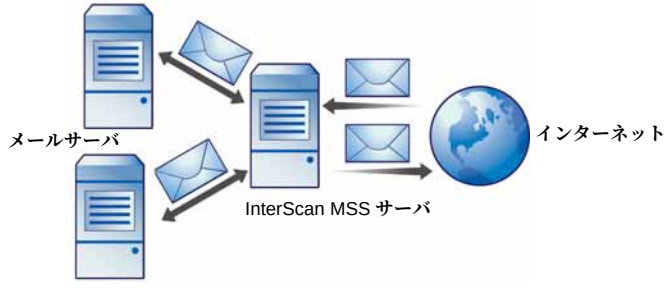


図 3-1. インストールトポロジ : ファイアウォールなし

注意： ファイアウォールなしでの InterScan MSS のインストールはお勧めしません。InterScan MSS のホストサーバをネットワークエッジに配置すると、サーバがセキュリティの脅威にさらされる可能性があります。

ファイアウォールの外側へのインストール

図 3-2. は、InterScan MSS をファイアウォールの外側にインストールする場合のインストールトポロジを示しています。

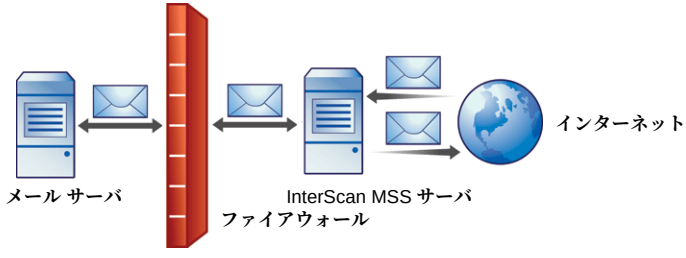


図 3-2. インストールトポロジ : ファイアウォールの外側

受信トラフィック

- 受信メールを受信する最初のサーバは、InterScan MSS にする必要があります。DNS サーバ上の MX レコードの設定変更を行い、SMTP ゲートウェイまたはファイアウォールの参照を、InterScan MSS サーバのアドレスまたは検索サービス間の負荷分散を実行するスイッチの参照に変更します。
- ローカルドメインのリレーのみを許可するように、リレードメインを設定します。

送信トラフィック

- ファイアウォールがない場合は、すべての送信メールを InterScan MSS に転送するように SMTP ゲートウェイを設定します。ファイアウォールがある場合は、すべての送信メールを InterScan MSS に転送するようにファイアウォール (プロキシベース) を設定して、メールが次のようにルーティングされるようにします。
  - 送信 SMTP メールは必ず InterScan MSS サーバに転送される。
  - 受信 SMTP メールは必ず InterScan MSS サーバ経由で着信する。
- 内部の SMTP ゲートウェイであらゆるドメインへの InterScan MSS 経由のリレーを許可するように、InterScan MSS を設定します。

ファイアウォールの内側へのインストール

図 3-3. は、InterScan MSS をファイアウォールの内側に配置する場合を示しています。

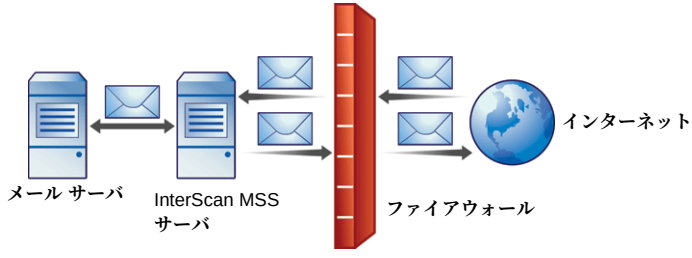


図 3-3. インストールトポロジ : ファイアウォールの内側

受信トラフィック

- プロキシベースのファイアウォールが構築されている場合は、ファイアウォールを次のように設定します。
  - 送信 SMTP メールは必ず、InterScan MSS サーバまたは検索サービス間の負荷分散を実行するスイッチに転送される。
  - 受信 SMTP メールは必ず InterScan MSS サーバ経由で着信する。
- パケットベースのファイアウォールが構築されている場合は、次のように設定します。
  - DNS サーバ上の MX レコードの設定変更を行い、SMTP ゲートウェイの参照を、InterScan MSS ホストサーバのアドレスの参照に変更します。
  - セキュアサブネットの管理用に InterScan MSS またはファイアウォールを設定している場合、InterScan MSS またはファイアウォールをポイントするように、MX レコードを設定します。
- ローカルドメイン宛に送られてくるメールを SMTP ゲートウェイまたは内部メールサーバ (Exchange IMS) に転送するように、InterScan MSS を設定します。
- リレーをローカルドメインのリレーのみに制限します。

送信トラフィック

- 送信メールを InterScan MSS サーバに転送するように、すべての内部 SMTP ゲートウェイを設定します。
- SMTP ゲートウェイを InterScan MSS に置き換えている場合は、送信メールを InterScan MSS サーバに転送するように、内部メールサーバ (Exchange IMS など) を設定します。
- すべての送信メール (ローカルドメイン以外のドメインを宛先とするもの) をファイアウォールに転送するか、または外部 DNS サーバを使用して配信するように、InterScan MSS を設定します。
- 内部 SMTP ゲートウェイであらゆるドメインへの InterScan MSS 経由のリレーを許可するように、InterScan MSS を設定します。

既存の SMTP ゲートウェイ上へのインストール

図 3-4 は、以前に SMTP ゲートウェイをホストしたサーバと同じサーバに InterScan MSS を集中インストールする場合を示しています。

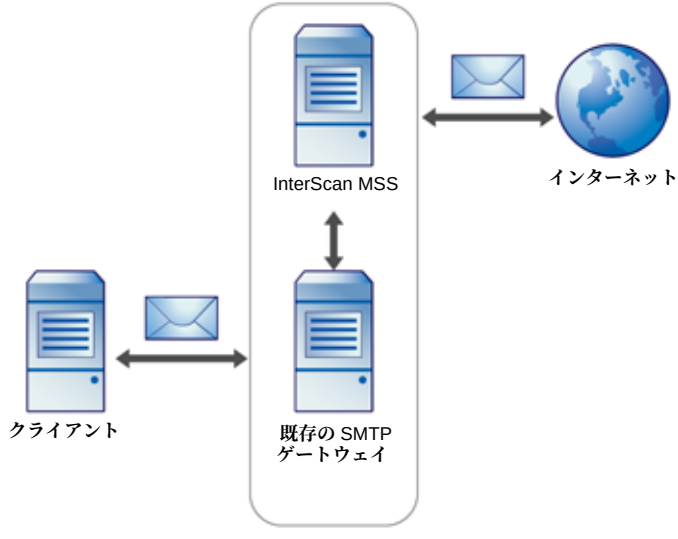


図 3-4.　インストールトポロジ : 既存の SMTP ゲートウェイ上

SMTP ゲートウェイ上で次の処理を実行します。

- ゲートウェイで、SMTP メールを転送するための新しい TCP/IP ポートを割り当てます。これには、他のサービスで使用されていないポートを割り当てる必要があります。
- 既存の SMTP ゲートウェイの設定で、このゲートウェイを新しく割り当てたポートにバインドします。それにより、ポート 25 が開放されます。
- InterScan MSS をインストールします。InterScan MSS はポート 25 にバインドされます。

受信トラフィック

- 受信メールを SMTP ゲートウェイおよび新しく割り当てたポートに転送するように、InterScan MSS を設定します。

送信トラフィック

- 送信メールを InterScan MSS サーバのポート 25 に転送するように、SMTP ゲートウェイを設定します。
- すべての送信メール (ローカル以外のドメインを宛先とするメッセージ) をファイアウォールに転送するか、または外部 DNS サーバを使用して配信するように、InterScan MSS を設定します。

DMZ 内へのインストール

InterScan MSS を DMZ にインストールすることもできます。

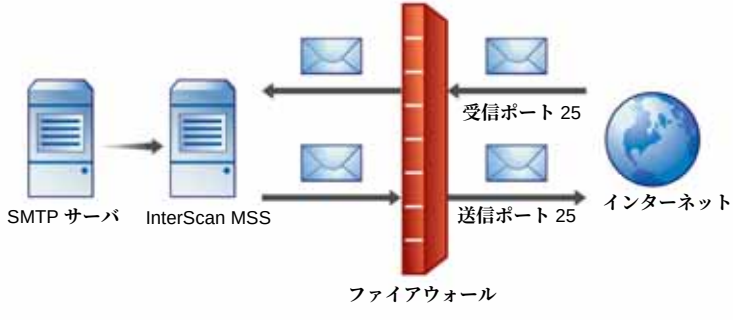


図 3-5.　インストールトポロジ :DMZ 内

受信トラフィック

- プロキシベースのファイアウォールが構築されている場合は、受信および送信 SMTP メールに対して DMZ から内部メールサーバへの送信のみ許容するようにファイアウォールを設定します。
- パケットベースのファイアウォールが構築されている場合は、ファイアウォールの設定変更を行い、DNS サーバ上の MX (Mail Exchange) レコードに指定されている SMTP ゲートウェイの参照を、InterScan MSS のホストサーバのアドレスまたは検索サービス間の負荷分散を実行するスイッチの参照に変更します。
- ローカルドメイン宛に送られてくるメールを SMTP ゲートウェイまたは内部メールサーバ (Exchange IMS) に転送するように、InterScan MSS を設定します。

送信トラフィック

- すべての送信メール (ローカルドメイン以外のドメインを宛先とするもの) をファイアウォールに転送するか、または外部 DNS サーバを使用して配信するように、InterScan MSS を設定します。
- 送信メールを InterScan MSS サーバに転送するように、すべての内部 SMTP ゲートウェイを設定します。

内部の SMTP ゲートウェイであらゆるドメインへの InterScan MSS 経由のリレーを許可するように、InterScan MSS を設定します。

インストールシナリオについて

InterScan MSS は、1 台のサーバにすべてのコンポーネントをインストールする集中インストール、または複数のサーバに分けてコンポーネントをインストールする分散インストールのいずれにも対応します。次の情報を参照し、適切なシナリオを選択してください。

集中インストール

集中インストールには、集中インストールの要件を満たす 1 台のサーバが必要です。InterScan MSS を集中インストールし、後からキャパシティを増やす必要がある場合は、検索サービスを簡単に追加インストールできます。

単一サーバ上に、次に示す InterScan MSS コンポーネントをすべてインストールできます。

- セントラルコントローラ
- InterScan MSS 管理データベース
- ポリシーサービス
- 検索サービス
- プライマリエンドユーザメール隔離サービスおよびエンドユーザメール隔離データベース
- MTA サービス
- IP フィルタサービス

注意： IP フィルタサービスを使用するには、InterScan MSS をエッジ MTA として配置する必要があります。

図 3-6. は、InterScan MSS の集中インストールが標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

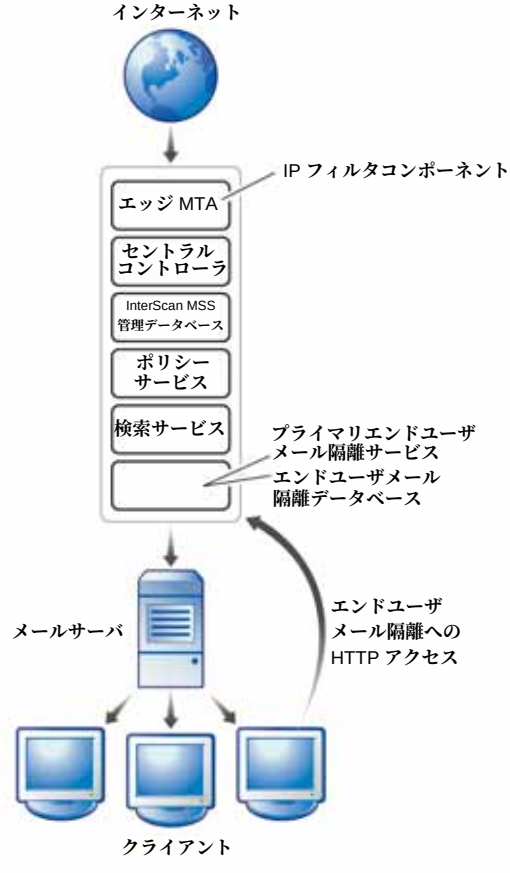


図 3-6.　集中インストール

集中インストールを実行するには

InterScan MSS およびエンドユーザメール隔離をインストールします。

複数の検索サービスのインストール

大規模企業の場合、単一サーバでは十分なメッセージスループットを確保できないことがあります。このような場合は、すべての InterScan MSS コンポーネントを 1 台のサーバにインストールしてから、追加のサーバに検索サービスコンポーネントをインストールすることができます。追加した検索サービスは、最初のサーバにインストールされたデータベースとポリシーサービスへのアクセスを共有します。このインストールシナリオでは、高レベルのメッセージスループットが確保されます。また、スパムメールの隔離アイテムをエンドユーザメール隔離で管理できるように、エンドユーザメール隔離コンソールをインストールすることも可能です。

複数の検索サービスとポリシーサービスのインストール

パフォーマンスを向上させるには、検索サービス、またはポリシーサービスと検索サービスの組み合わせをインストール後に追加します。

図 3-7. は、InterScan MSS の集中インストールに 2 つの検索サービスを追加した構成が標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

エッジ MTA と InterScan MSS 検索サービス間にレイヤ 4 スイッチを配置すると、負荷を分散させることができます。

注意： IP フィルタサービスを使用するには、InterScan MSS をエッジ MTA として配置する必要があります。

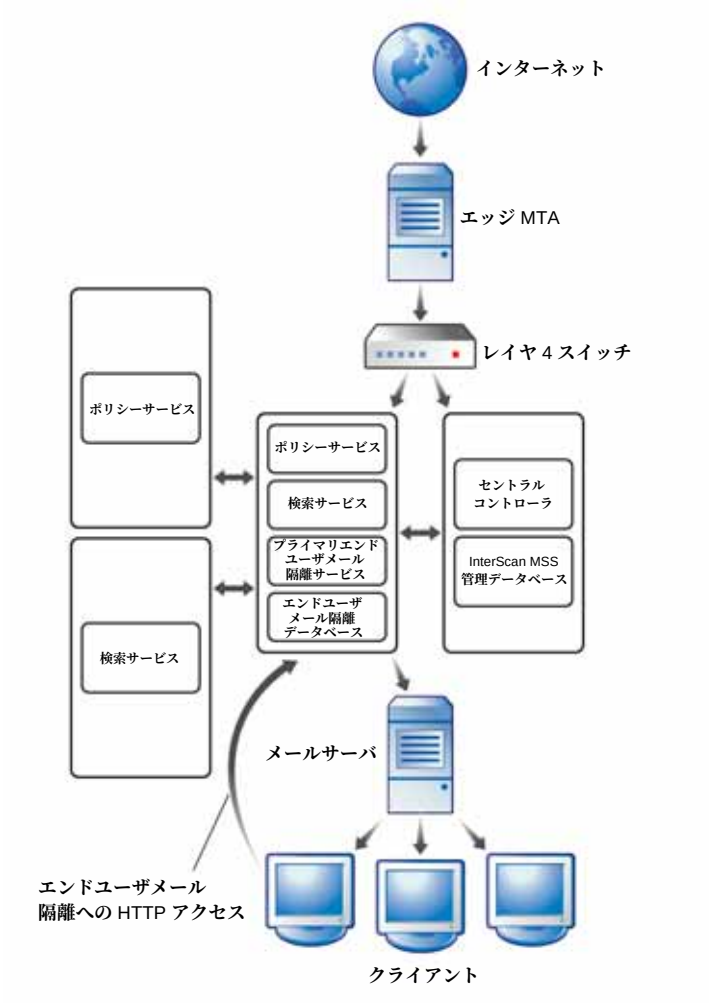


図 3-7.　複数の検索サービスおよびポリシーサービスのインストール

複数の検索サービスのインストールを実行するには

1. 1 台のコンピュータに、InterScan MSS とエンドユーザメール隔離をインストールします。
2. 別のコンピュータに、必要な検索サービスとポリシーサービスをインストールします。

注意： ポリシーサービスは、常に検索サービスのインストール先のコンピュータにインストールする必要があります。ポリシーサービスは、必要な数だけ起動することができます。

3. InterScan MSS 管理コンソールを開いて初期設定を行った後、[概要]→[システム] 画面に移動します。
4. 有効にする検索サービスまたはポリシーサービスに対して [開始] をクリックします。

複数のエンドユーザメール隔離サービスのインストール

大量のスパムメールを受信する企業で、ユーザがスパムメールにアクセスできるようにするには、エンドユーザメール隔離の複数のセカンダリサーバまたはセカンダリデータベース、あるいはこの両方をインストールします。

注意： エンドユーザメール隔離サーバとエンドユーザメール隔離データベースは 8 つまでインストールできます。

図 3-8. は、InterScan MSS の集中インストールに、独立したプライマリエンドユーザメール隔離サーバと追加のセカンダリエンドユーザメール隔離サーバ (負荷分散のための Apache サービスを含む) および分散エンドユーザメール隔離データベースを加えた構成が、標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

注意： IP フィルタサービスを使用するには、InterScan MSS をエッジ MTA として配置する必要があります。

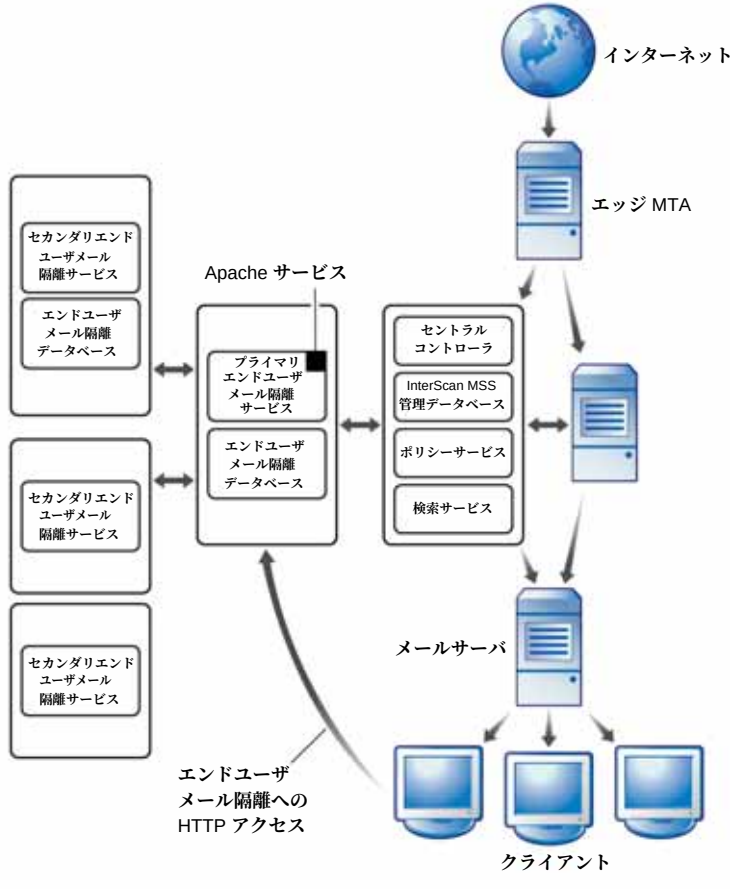


図 3-8.　複数のエンドユーザメール隔離サービスのインストール

複数のエンドユーザメール隔離サービスのインストールを実行するには

1. 1 台のコンピュータに、InterScan MSS をインストールします。
2. 別のコンピュータに、エンドユーザメール隔離サービスを 1 つインストールします。これはプライマリエンドユーザメール隔離サービスになります。
3. プライマリエンドユーザメール隔離サービスと通信できるその他のコンピュータに、追加のエンドユーザメール隔離サービスをインストールします。エンドユーザメール隔離サービスに、少なくとも 1 つのエンドユーザメール隔離データベースをインストールする必要があります。また、パフォーマンスを向上させるために追加のエンドユーザメール隔離データベースをインストールすることもできます。エンドユーザメール隔離データベースは、エンドユーザメール隔離サービスの実行元のコンピュータまたは別のコンピュータにインストールできます。

   注意： インストール後に負荷分散を実行しているのは、プライマリエンドユーザメール隔離サービスにインストールされた Apache サービスだけです。

4. InterScan MSS 管理コンソールを開いて初期設定を行った後、[概要]→[システム] 画面に移動します。
5. 有効にするエンドユーザメール隔離サービスに対して [開始] をクリックします。

エンドユーザメール隔離を配置する際のその他の検討事項

社内のエンドユーザが Web ベースのエンドユーザメール隔離にアクセスするには、サーバへの HTTPS アクセスが必要です。また、エンドユーザメール隔離コンポーネントをホストするサーバは、InterScan MSS が隔離したアイテムの情報の格納に使用する、エンドユーザメール隔離データベースに接続できる必要もあります。

つまり、エンドユーザメール隔離とネットワーク上のエンドユーザコンピュータの間にファイアウォールが存在する場合、そのファイアウォールは内部アドレスからの HTTPS 接続をブロックしない種類のものであるか、または HTTPS トラフィックを許可するように設定されていなければなりません。

Web ベースの隔離とデータベースは、InterScan MSS とは別のサーバにインストールすることもできます。この場合は、InterScan MSS と他のサーバとの間に存在するファイアウォールに対しては、InterScan MSS と他のサーバとの間のデータベース接続を許可するように設定する必要があります。

サーバ間の通信

内部ファイアウォールを使用する場合は、InterScan MSS、エンドユーザメール隔離、およびデータベース間の通信を許可するようにファイアウォールを設定します。たとえば、1 つのシステムにエンドユーザメール隔離サービスをインストールし、別のシステムにデータベースをインストールする場合に、この 2 つのシステム間にファイアウォールが存在するならば、データベースへの接続を許可するようにファイアウォールを設定する必要があります。

複雑な分散インストール

非常に規模の大きな企業では、分散インストールを選択することをお勧めします。このシナリオでは、コンポーネントごとにインストール要件を満たすサーバが必要です。分散インストールでは、InterScan MSS とエンドユーザメール隔離の各コンポーネントを異なるサーバにインストールします。1 台のサーバにデータベースを、もう 1 台のサーバにセントラルコントローラをインストールし、他の複数のサーバにポリシーサービスと検索サービスの両方をインストールできます。

また、スパムメールの隔離アイテムをユーザが管理できるように、複数のエンドユーザメール隔離コンソールをインストールすることも可能です。同様に、複数のエンドユーザメール隔離データベースをインストールして、エンドユーザメール隔離パフォーマンスを強化することもできます。追加の検索サービスとエンドユーザメール隔離サービスは、随時インストールできます。

注意： エンドユーザメール隔離サービスとエンドユーザメール隔離データベースは 8 つまでインストールできます。

高スループットが求められる環境では、各 InterScan MSS コンポーネントを個別のコンピュータにインストールし、複数の検索サービス、エンドユーザメール隔離サービス、およびデータベースを配置できます。

注意： エンドユーザメール隔離データベースを InterScan MSS の管理データベースと混同しないようにしてください。InterScan MSS の配置ごとに、エンドユーザメール隔離データベースは複数インストールできますが、InterScan MSS 管理データベースは 1 つしかインストールできません。

図 3-9. は、InterScan MSS と複数の検索サービス、ポリシーサービス、およびエンドユーザメール隔離サービス (負荷分散用 Apache サービスを含む) を一元化した構成が、標準のメッセージングネットワークトポロジにどのように適合するかを示しています。

注意： インストール後に負荷分散を実行しているのは、プライマリエンドユーザメール隔離サービスにインストールされた Apache サービスだけです。

ポリシーサービスは、常に検索サービスと同じコンピュータにインストールする必要があります。必要に応じて、いくつものポリシーサービスを起動することができます。

注意： IP フィルタサービスを使用するには、InterScan MSS をエッジ MTA として配置する必要があります。

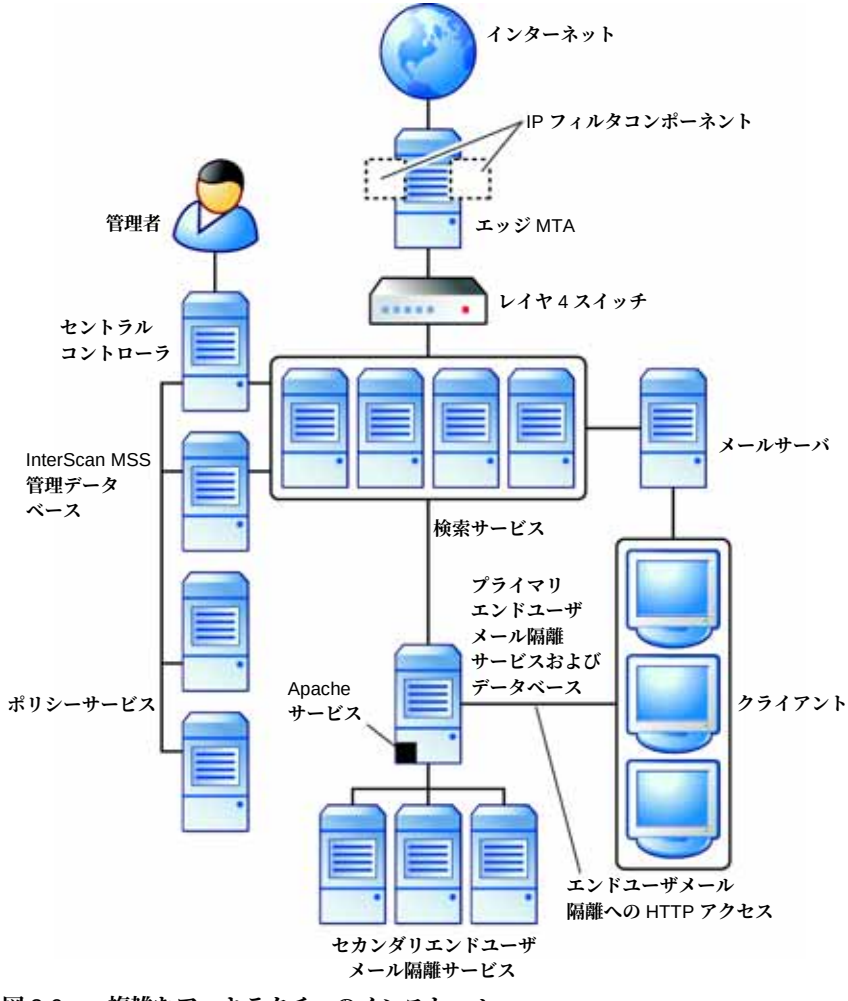


図 3-9.　複雑なアーキテクチャのインストール

WAN へのインストール

広域ネットワーク (WAN) に複数のサイトがある場合、InterScan MSS コンポーネントを分散してインストールし、さまざまな方法で配置できます。

ヒント： コンポーネント間で適切な通信が行われるようにするために、サイトごとに少なくとも 1 つのセントラルコントローラコンポーネントと 1 つの InterScan MSS 管理データベースコンポーネントを配置することをお勧めします。そのためには、各サイトで InterScan MSS を新規にインストールし、複数の検索サービスまたはエンドユーザメール隔離をインストールする場合には、インストール後にコンポーネントを追加します。

Trend Micro Control Manager

すべての InterScan MSS サーバ (セントラルコントローラがインストールされているサーバ) を簡単に管理できるようにするには、Control Manager サーバをインストールすることをお勧めします。このシナリオでは、2 つの Control Manager サーバですべてのサイトが管理され、Control Manager 間の通信によってデータベース情報が複製されます。

図 3-10. は、複数サイトの WAN での配置を示しています。

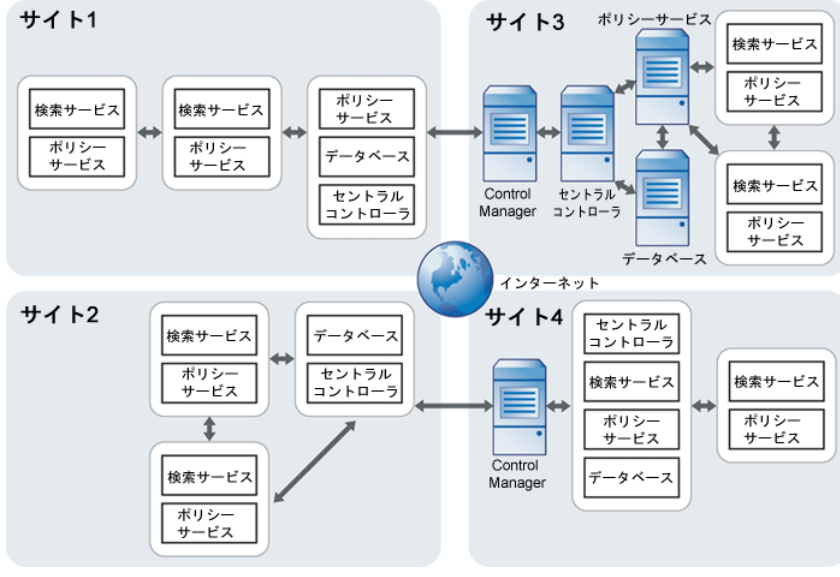


図 3-10.　WAN での配置

この配置の場合、各サイトの違いは次のようになります。

- **サイト 1** — セントラルコントローラ、InterScan MSS 管理データベース、およびポリシーサービスを備える InterScan MSS サーバ + ポリシーサービスが有効に設定された 2 つの InterScan MSS 検索サービス。
- **サイト 2** — セントラルコントローラ、InterScan MSS 管理データベース、およびポリシーサービスを備える InterScan MSS サーバ + ポリシーサービスが有効に設定された 2 つの InterScan MSS 検索サービス (フォールトトレランス用)。
- **サイト 3** — InterScan MSS セントラルコントローラ + InterScan MSS 管理データベース + 単一のポリシーサービスのみ + ポリシーサービスが有効に設定された 2 つの InterScan MSS 検索サービス (フォールトトレランス用)。
- **サイト 4** — セントラルコントローラと InterScan MSS 管理データベースを備える InterScan MSS サーバ + ポリシーサービスが有効に設定された InterScan MSS 検索サービス。

WAN での配置構成におけるフォールトトレランスとフェイルオーバー

このシナリオでは、4 つのサイトのうち 3 つはポリシーサービスをインストールした複数の検索サービスを使用します。ポリシーサービスは、キャッシュされた InterScan MSS 設定に InterScan MSS 管理データベースからアクセスできます。検索サービスはポリシーサービスが機能停止になっても、別の有効なポリシーサービスを使用することができます。したがって、1 つのポリシーサービスが停止したり、セントラルデータベースとの通信が切断されたりしても、検索サービスは継続して機能し、InterScan MSS サーバに接続されている有効なポリシーサービスを使用してメールの処理を続行します。図 3-11. を参照してください。

各サイトには、それぞれ専用のセントラルコントローラとデータベースサーバがあり、それらはいずれも 2 つの Control Manager サーバにレポートを返します。それぞれの Control Manager サーバは、その Control Manager サーバに登録されているすべての InterScan MSS 配置間で InterScan MSS 管理データベース内の InterScan MSS の設定を複製できます。1 つの InterScan MSS 管理データベースが壊れて動作しなくなっても、複製を使用して復元できます。

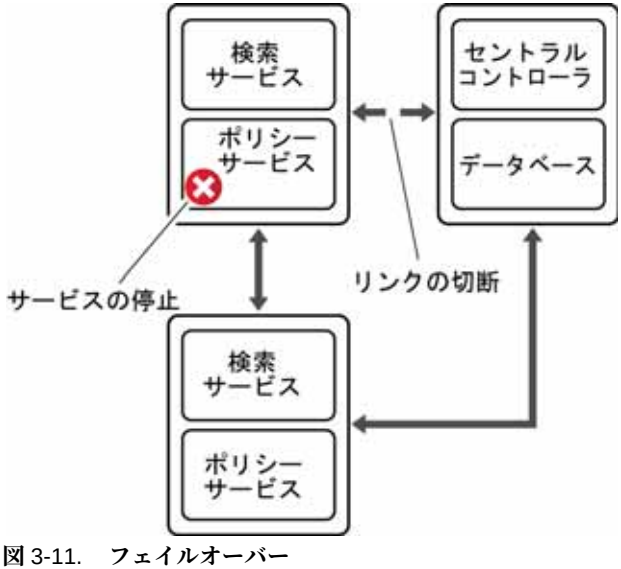


図 3-11.　フェイルオーバー

IP フィルタ

IP プロファイラは、カスタム設定を使用して、各種の攻撃を示すメールメッセージに対応します。

IP フィルタ機能を付加した InterScan MSS の配置

IP フィルタ、すなわち IP プロファイラと NRS は、どちらも IP レベルで接続をブロックします。IP プロファイラは、カスタム設定を使用して、各種の攻撃を示すメールメッセージに対応します。NRS は、Trend Micro Threat Reputation Network の情報を使用して、SMTP 接続を開始しようとしているコンピュータが既知のスパムメール送信者かどうかを判定します。

注意： ネットワークエッジから InterScan MSS 接続までの区間でアドレスが変更されないようにする必要があります。つまり、InterScan MSS とネットワークエッジの間にファイアウォールが存在する場合、そのファイアウォールは接続 IP アドレスを変更しないタイプのものであるか、または変更しないように設定されていなければなりません。

たとえば、InterScan MSS が常にルータからの SMTP 接続を受け入れる場合、IP フィルタは機能しません。なぜなら、このアドレスは受信するすべてのメッセージで同じになり、IP フィルタソフトウェアは、SMTP セッションの開始元が既知のスパムメール送信者であるかどうか判断できなくなるためです。

IP フィルタ機能を備える InterScan MSS の配置の詳細については、本書の「IP フィルタのインストール」および管理者ガイドの「IP フィルタサービス」を参照してください。

フェイルオーバーについて

表 3-3 は、InterScan MSS コンポーネントの障害時に発生する問題点、および InterScan MSS の保護機能を維持したまま実行するフェイルオーバーの方法を示しています。WAN での配置構成におけるフェイルオーバーの詳細については、74 ページの「WAN での配置構成におけるフォールトトレランスとフェイルオーバー」を参照してください。

障害のあるコンポーネント	予測される結果	推奨フェイルオーバー
検索サービスが起動しない、または切断される	1. InterScan MSS は検索サービスの再起動を試行します。 2. サービスが、指定した時間以内に起動できない場合には、イベント通知が送信されます。	負荷分散とフェイルオーバーのために、複数の検索サービスをインストールします。詳細については、92 ページの「検索サービスとエンドユーザメール隔離サービス / データベースの複数インストール」を参照してください。
ポリシーサービスが起動しない、または InterScan MSS サーバとの通信に問題が発生する	1. 停止したポリシーサービスを使用している検索サービスは、有効なポリシーサービスがある場合、そのサービスへ切り替えます。 2. InterScan MSS はポリシーサービスの再起動を試行します。 3. サービスが、指定した時間以内に起動または再接続できない場合には、イベント通知が送信されます。	負荷分散とフェイルオーバーのために、複数の検索サービスをインストールします。詳細については、92 ページの「検索サービスとエンドユーザメール隔離サービス / データベースの複数インストール」を参照してください。
InterScan MSS 管理データベースが動作しない	1. InterScan MSS サーバは、動作を続行します。 2. サービスが、指定した時間以内に起動できない場合には、イベント通知が送信されます。	管理データベースのバックアップを定期的に作成します。 詳細については、http://www.microsoft.com/ja/jp/ にアクセスしてください。

表 3-3.　フェイルオーバーの構成

障害のあるコンポーネント	予測される結果	推奨フェイルオーバー
エンドユーザメール隔離データベースが動作しない	1. エンドユーザメール隔離管理コンソールにエラーメッセージが表示されます。 2. サービスが、指定した時間以内に起動できない場合には、イベント通知が送信されます。	エンドユーザメール隔離データベースのバックアップを定期的に作成します。 バックアップと復元の詳細については、http://www.microsoft.com/ja/jp/ にアクセスしてください。
LDAP サーバが動作しない	1. エンドユーザメール隔離にログインする際、エンドユーザメール隔離管理コンソールにエラーメッセージが表示されます。 2. IP プロファイラは、LDAP 設定を使用しません。 3. LDAP が切断された場合、ポリシールートで LDAP グループが指定されていると、InterScan MSS はキャッシュ済みの LDAP エントリ (使用可能な場合) をポリシー一致の実行時に使用して、正常に動作を続行します。また、切断に関するイベント通知も、指定されたアドレスへ自動的に送信されます。送信先のアドレスは、[管理]→[通知]→[通知設定] の順に選択して指定します。 **注意** : LDAP の切断の通知はバックエンドで自動的に送信されるので、この通知は管理コンソールで設定することはできません。	次の手順で、セカンダリ LDAP サーバを有効にします。 1. [管理]→[接続] を選択します。 2. [LDAP] タブをクリックします。 3. [有効]、[LDAP2] 横のチェックボックスをオンにし、必要な情報を入力します。 LDAP サーバでフォールトトレランス機能を有効にすることもお勧めします。

表 3-3. フェイルオーバーの構成

第 4 章

インストールとアップグレード

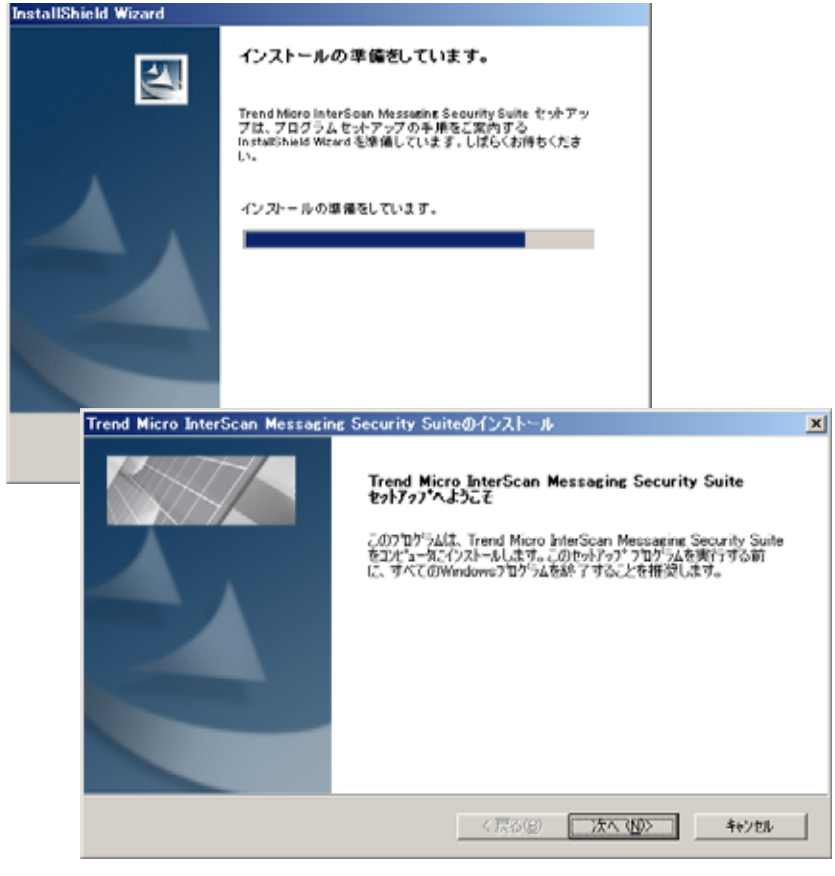
この章では、さまざまな状況での Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) のインストールおよびアンインストール方法と、InterScan MSS のバックアップ、復元、アップグレードの各手順について説明します。

- 80 ページの「集中インストール」
- 92 ページの「検索サービスとエンドユーザメール隔離サービス / データベースの複数インストール」
- 104 ページの「複雑な分散インストール」
- 105 ページの「サイレントインストール」
- 108 ページの「InterScan MSS 5.18 からのアップグレード」
- 113 ページの「アップグレード後のロールバック」
- 114 ページの「アンインストールの実行」

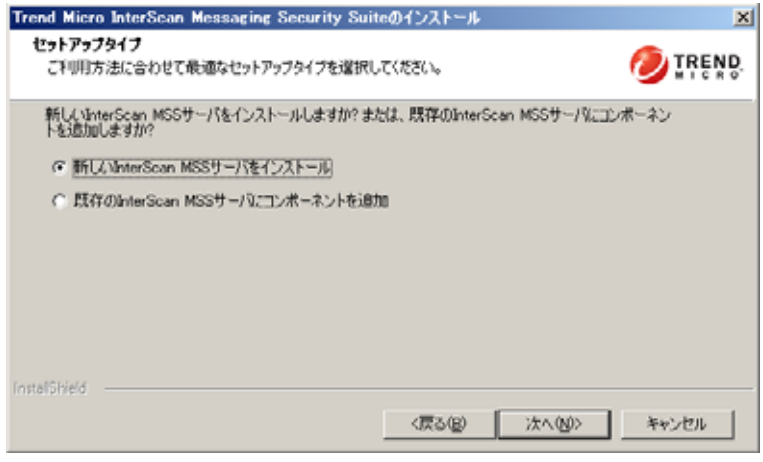
集中インストール

基本的なインストールを実行するには

1. Setup.exe をダブルクリックします。[インストールの準備をしています。] 画面に続いて、[セットアップへようこそ] 画面が表示されます。

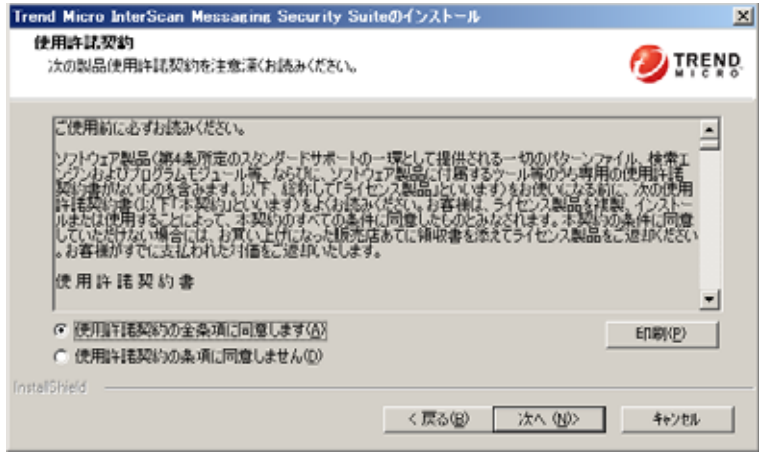


2. [次へ] をクリックします。[セットアップタイプ] 画面が表示されます。



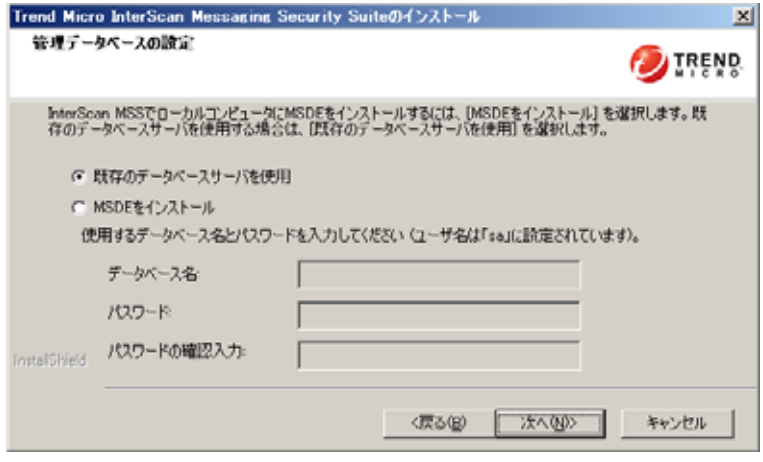
3. [新しい InterScan MSS サーバをインストール] を選択します。

4. [次へ] をクリックします。[使用許諾契約] 画面が表示されます。



5. 使用許諾書をよく読んでから、[使用許諾契約の全条項に同意します] を選択します。

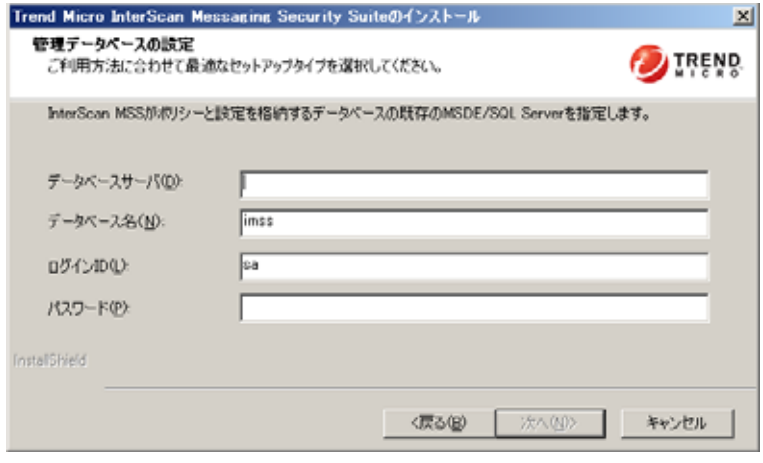
6. [次へ] をクリックします。[管理データベースの設定] 画面が表示されます。



既存のデータベースサーバを使用するには

a. [既存のデータベースサーバを使用] を選択します。

b. [次へ] をクリックします。既存のデータベースサーバに関する必要な情報を入力します。

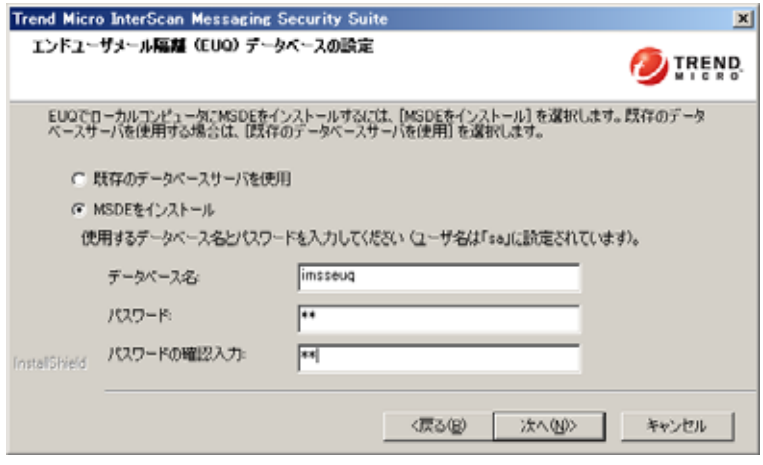


注意： 対象コンピュータにデータベースサーバが複数存在する場合は、IP アドレスまたはホスト名を入力します。

このサーバに Microsoft SQL Server Desktop Engine (MSDE) データベースをインストールするには

a. [MSDE をインストール] を選択します。

b. MSDE「sa」ユーザアカウントのデータベース名とパスワードを入力します。



ヒント： MSDE 2000 には次の制限が適用されます。
- データ量 2GB
- 同時ユーザ接続または作業負荷数 5

1 日のメールトラフィックが 30,000 件を上回る場合や、InterScan MSS エンドユーザメール隔離を使用している場合、MSDE を使用しないようにしてください。これは、レポートとログクエリ結果の保存用に十分な空き領域を確保する必要があるためです。

注意： 以下の問題を回避するために、データベースサービスの TCP/IP プロトコルを有効にします。
1. インストール時に IP アドレスを使用して既存のデータベースに接続できない。
2. セントラルコントローラの管理コンソールを開けない。

7. [次へ] をクリックします。[インストール先の選択] 画面が表示されます。

8. インストール先のディレクトリを変更するには、[参照] をクリックして必要なディレクトリを選択します。

注意： Windows 2003 x64 プラットフォームの場合、InterScan MSS 7.0 は次のディレクトリにはインストールできません。

C:¥program Files¥Trend Micro¥imss

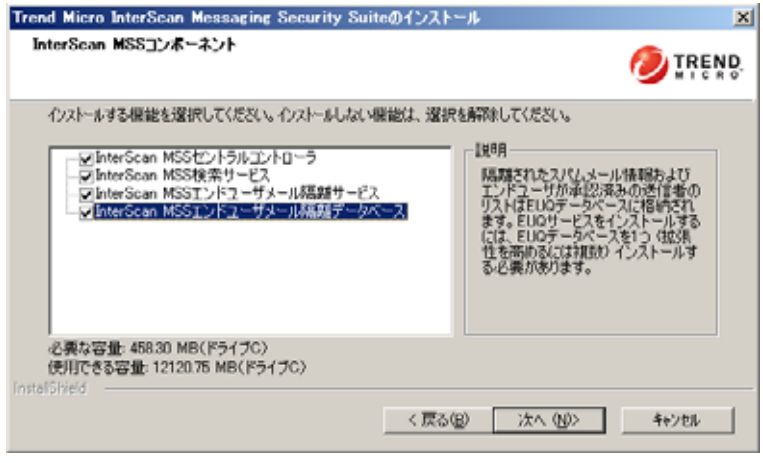
Windows 2003 x64 プラットフォームでこのディレクトリに配置できるのは、x64 プログラムに限られます。

x64 プラットフォームでは、次のディレクトリに InterScan MSS をインストールしてください。

C:¥program Files (x86)¥Trend Micro¥imss

---

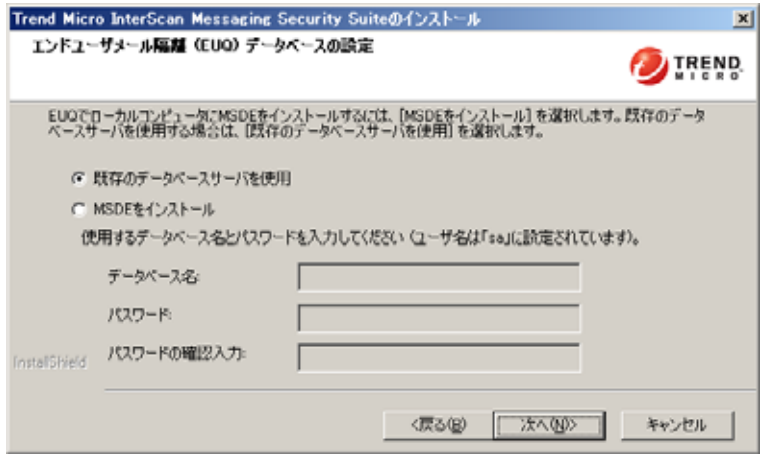
9. [次へ] をクリックします。[InterScan MSS コンポーネント] 画面が表示されます。



10. 必要なコンポーネントを選択します。

- InterScan MSS **セントラルコントローラ** — セントラルコントローラには、Web サーバコンポーネントが含まれ、このコンポーネントにより、管理コンソールを Web ブラウザで表示できるようになります。管理者はこの管理コンソールを使用して、InterScan MSS の設定と制御を行うことができます。
- InterScan MSS **検索サービス** — 検索サービスは、SMTP および POP3 のメッセージングトラフィックを受け入れて、ポリシーサーバにポリシーを要求し、該当するポリシーに基づいてメッセージを評価し、評価結果に基づいて適切な処理を実行します。
- InterScan MSS **エンドユーザメール隔離サービス** — プライマリエンドユーザメール隔離サーバには、InterScan MSS の管理コンソールと同様に Web ベースのコンソールが生成されるため、ユーザは、処理されたスパムメールの表示、削除、または再送を行うことができます。
- InterScan MSS **エンドユーザメール隔離データベース** — エンドユーザメール隔離データベースには、隔離されたスパムメールの情報、およびエンドユーザの承認済み送信者リストが格納されます。エンドユーザメール隔離をインストールする場合は、エンドユーザメール隔離データベース (スケーラビリティを高める場合は複数のデータベース) もインストールする必要があります。

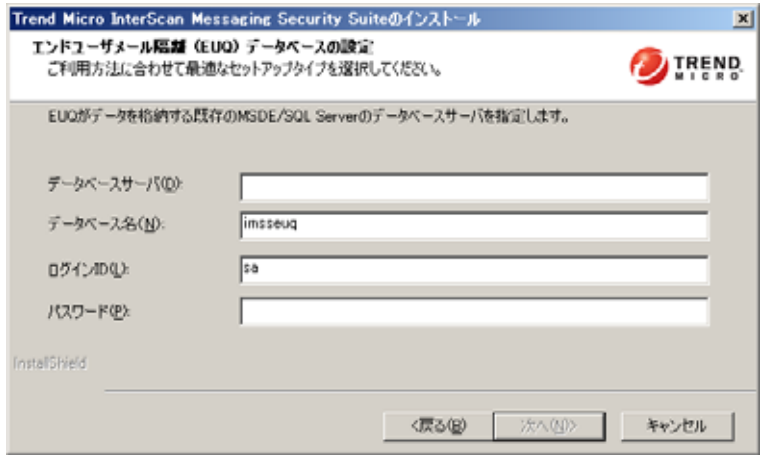
11. [次へ] をクリックします。[InterScan MSS エンドユーザメール隔離データベース] オプションを選択した場合は、[エンドユーザメール隔離 (EUQ) データベースの設定] 画面が表示されます。



既存のデータベースサーバを使用するには

a. [既存のデータベースサーバを使用] を選択します。

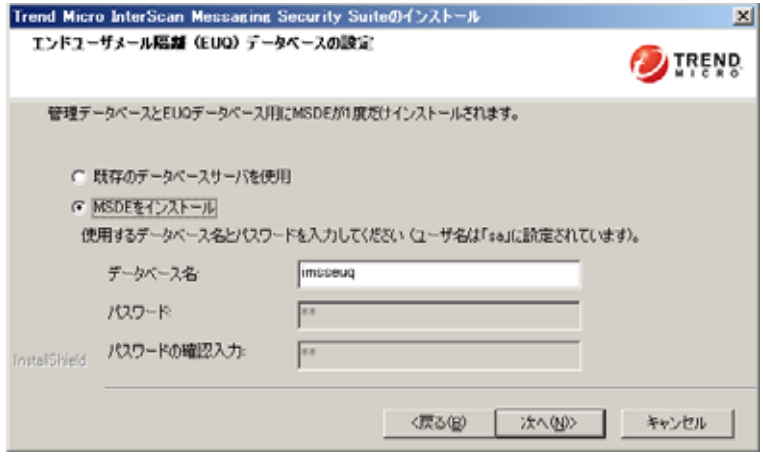
b. [次へ] をクリックします。既存のデータベースサーバに関する情報を入力します。



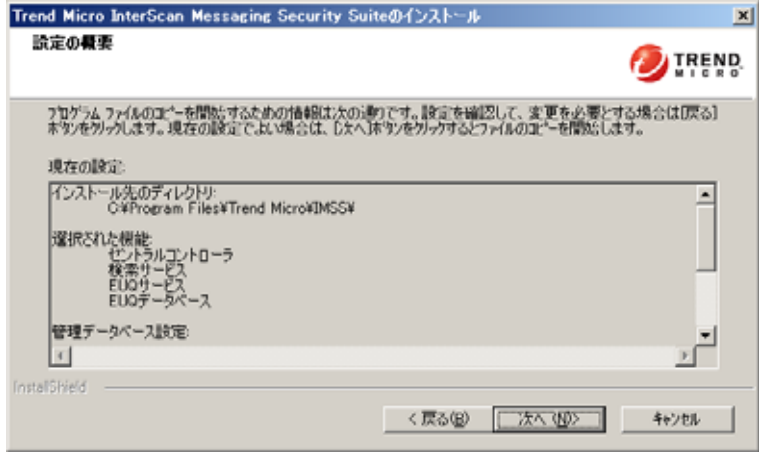
このサーバに MSDE データベースをインストールするには

a. [MSDE をインストール] を選択します。

b. MSDE「sa」ユーザアカウントのエンドユーザメール隔離データベース名とパスワードを入力します。



12. [次へ] をクリックします。[設定の概要] 画面が表示されます。



13. 選択したコンポーネントと、定義した設定を確認します。[次へ] をクリックします。[セットアップ ステータス] 画面が表示され、インストールが開始されます。

14. [次へ] をクリックします。[InstallShield Wizard の完了] 画面が表示されます。

15. [はい、今すぐコンピュータを再起動します。] を選択します。

16. [完了] をクリックします。

検索サービスとエンドユーザメール隔離サービス / データベースの複数インストール

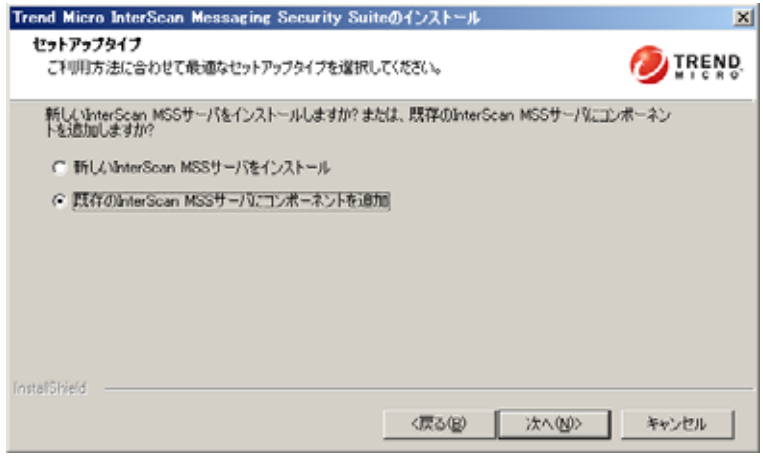
この項では、複数の検索サービスとエンドユーザメール隔離サービスをインストールする方法について説明します。また、InterScan MSS のコンポーネントがすでに存在するコンピュータにコンポーネントを追加インストールする場合と、既存の InterScan MSS コンポーネントが存在しないコンピュータにコンポーネントを新規インストールする場合の違いについても説明します。

以前にインストールされたコンポーネントが存在しない場合のコンポーネントの追加

以前にインストールされたコンポーネントが存在しないコンピュータに検索サービスまたはエンドユーザメール隔離サービス / データベースを追加するには

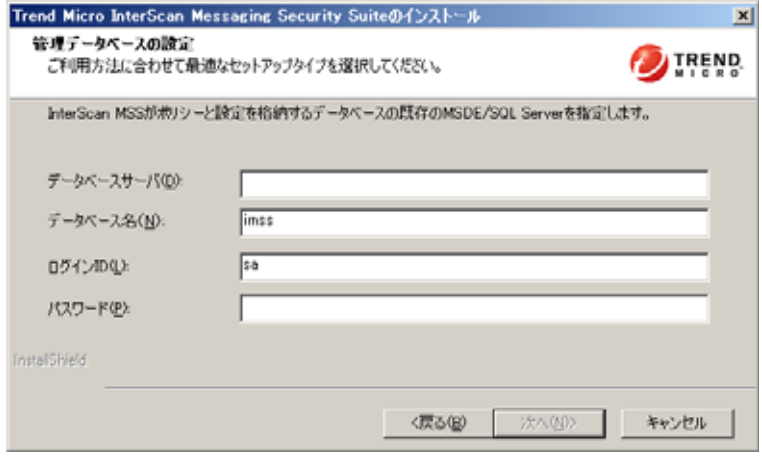
1. Setup.exe をダブルクリックします。[インストールの準備をしています。] 画面に続いて、[セットアップへようこそ] 画面が表示されます。

2. [次へ] をクリックします。[セットアップタイプ] 画面が表示されます。



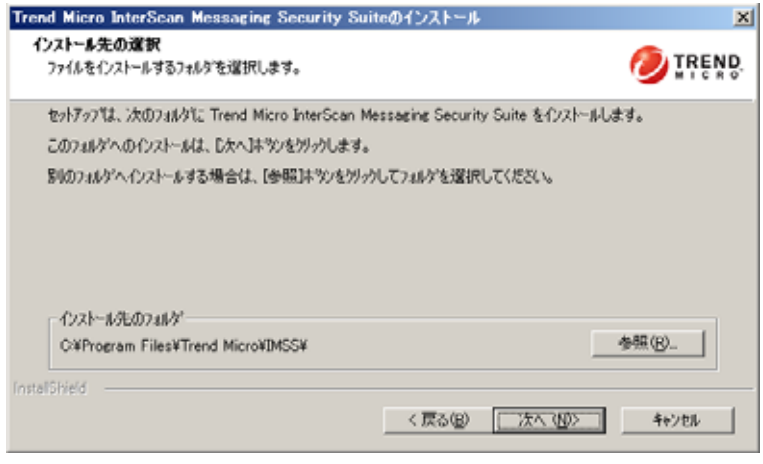
3. [既存の InterScan MSS サーバにコンポーネントを追加] を選択します。

4. [次へ] をクリックします。[管理データベースの設定] 画面が表示されます。



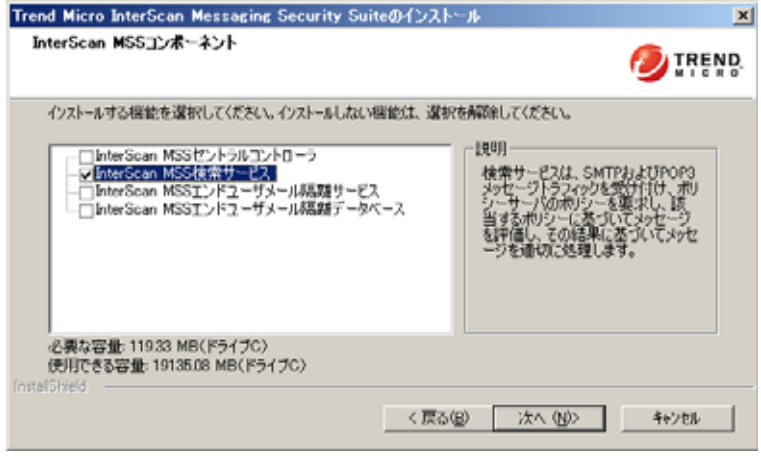
5. 管理データベースに関する必要な情報を入力します。

6. [次へ] をクリックします。[インストール先の選択] 画面が表示されます。



7. インストール先のパスを指定します。

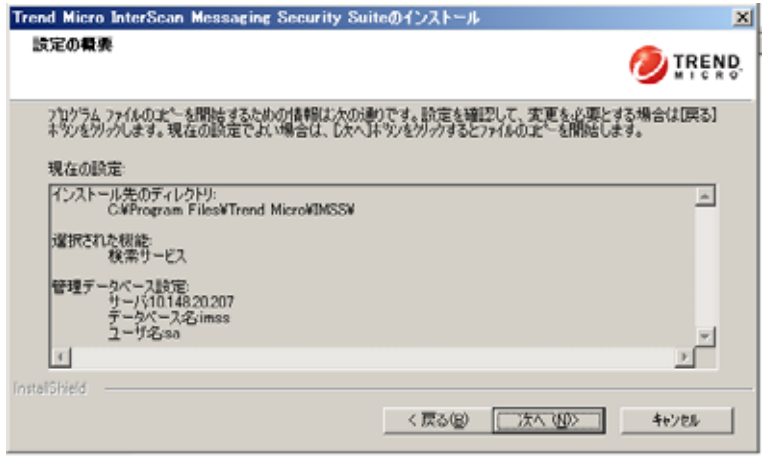
8. [次へ] をクリックします。[InterScan MSS コンポーネント] 画面が表示されます。



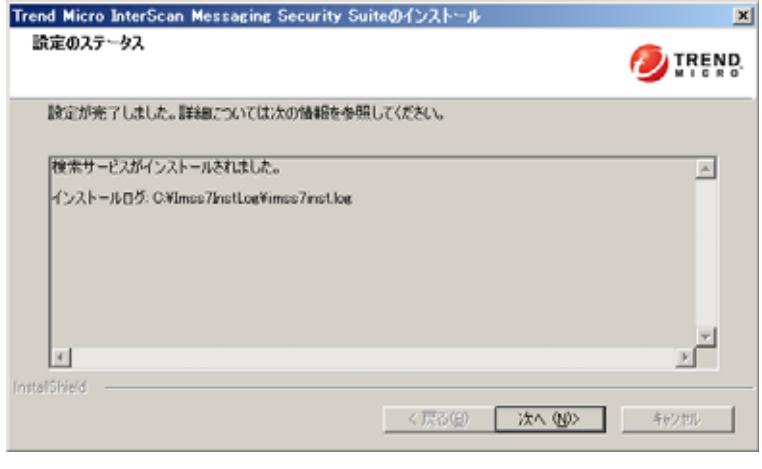
追加の InterScan MSS 検索サービスをインストールするには

a. [InterScan MSS 検索サービス] コンポーネントを選択します。

b. [次へ] をクリックします。[設定の概要] 画面が表示されます。



c. 設定を確認して [次へ] をクリックします。[セットアップステータス] 画面が表示されます。

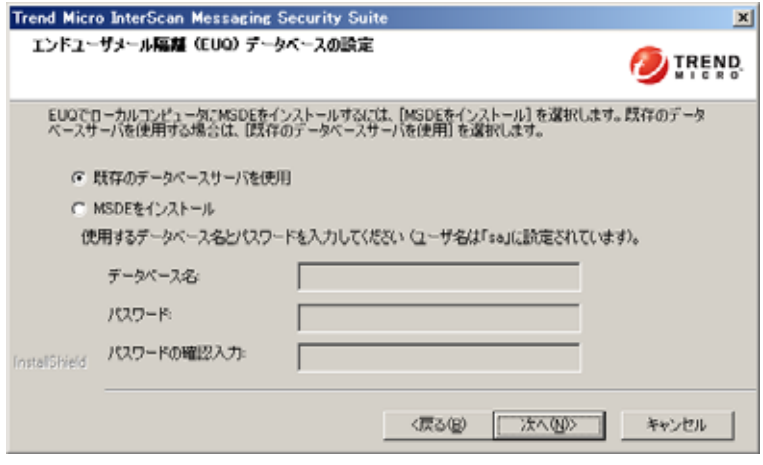


d. [次へ] をクリックします。ファイルがインストールされます。

追加のエンドユーザメール隔離サービスまたはエンドユーザメール隔離データベース、あるいはこの両方をインストールするには

a. [InterScan MSS エンドユーザメール隔離サービス] または [InterScan MSS エンドユーザメール隔離データベース]、あるいはこの両方を選択します。

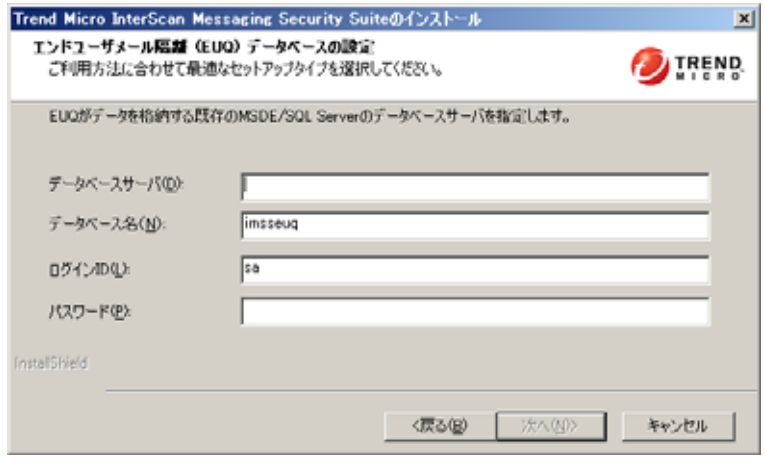
b. [次へ] をクリックします。[エンドユーザメール隔離 (EUQ) データベースの設定] 画面が表示されます。



既存のデータベースサーバにエンドユーザメール隔離データベースをインストールするには

i. [既存のデータベースサーバを使用] を選択します。

ii. [次へ] をクリックします。[エンドユーザメール隔離 (EUQ) データベースの設定] 画面が表示されます。



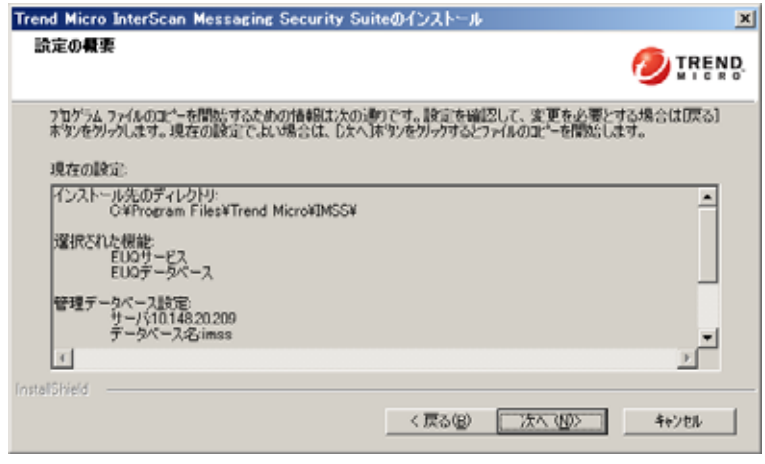
iii. 既存のデータベースサーバに関する情報を入力します。

このサーバに MSDE データベースをインストールするには

i. [MSDE をインストール] を選択します。

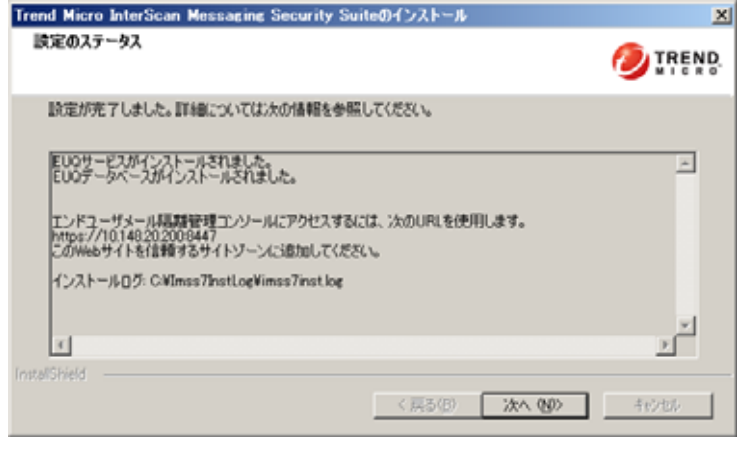
ii. MSDE「sa」ユーザアカウントのエンドユーザメール隔離データベース名とパスワードを入力します。

c. [次へ] をクリックします。[設定の概要] 画面が表示されます。



d. 選択したコンポーネントと、定義した設定を確認します。

e. [次へ] をクリックします。[セットアップ ステータス] 画面が表示されます。



9. [次へ] をクリックします。[InstallShield Wizard の完了] 画面が表示されます。

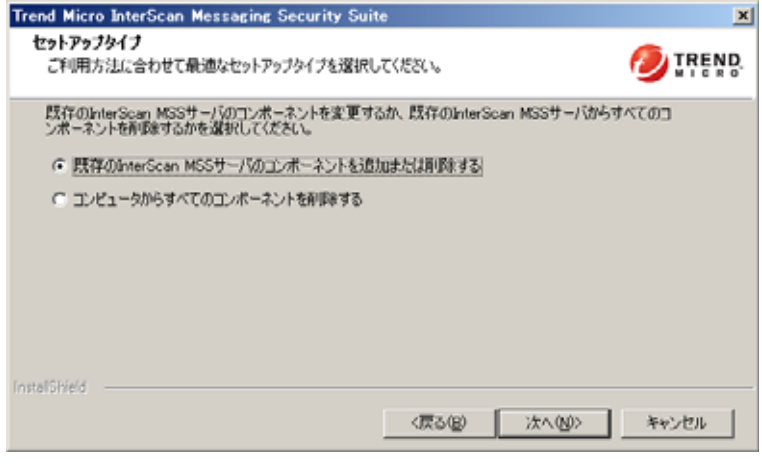
10. [はい、今すぐコンピュータを再起動します。] を選択します。[完了] をクリックします。

注意： 追加のエンドユーザメール隔離データベースのインストールを選択した場合は、セントラルコントローラの $IMSS_HOME¥bin¥ ディレクトリに移動して、コマンドラインで euqtrans.bat を実行し、元のエンドユーザメール隔離データベースからすべてのデータベースにデータを再配信します。

以前にインストールされたコンポーネントが存在する場合のコンポーネントの追加

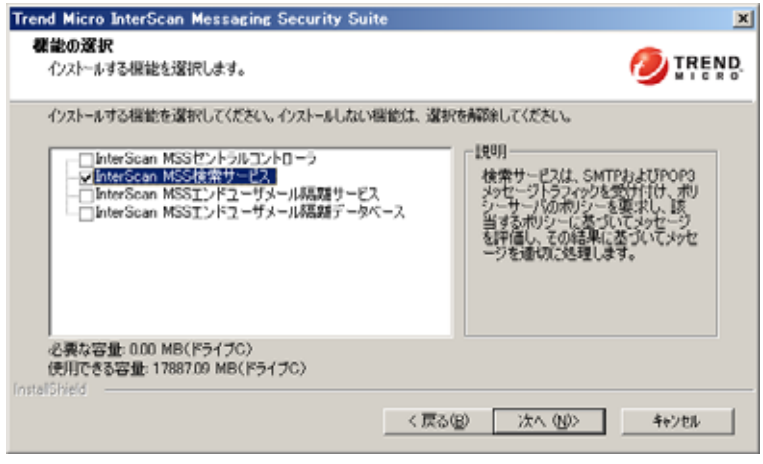
以前にインストールされた InterScan MSS コンポーネントが存在するコンピュータに検索サービスまたはエンドユーザメール隔離サービス / データベースを追加するには

1. Setup.exe をダブルクリックします。[インストールの準備をしています。] 画面に続いて、[セットアップへようこそ] 画面が表示されます。
2. [次へ] をクリックします。[セットアップタイプ] 画面が表示されます。



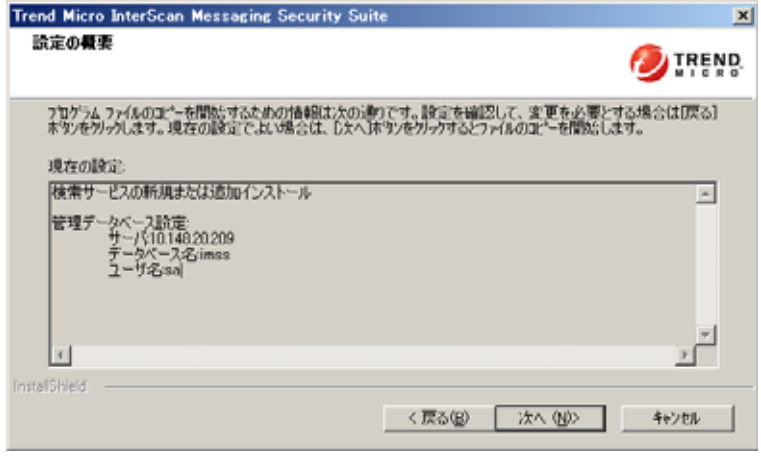
3. [既存の InterScan MSS サーバのコンポーネントを追加または削除する] を選択します。

4. [次へ] をクリックします。[機能の選択] 画面が表示されます。



5. 追加するコンポーネントを選択します。

6. [次へ] をクリックします。[設定の概要] 画面が表示されます。追加のエンドユーザメール隔離サービスまたはデータベースのインストールを選択した場合は、[設定の概要] 画面が表示される前に、エンドユーザメール隔離データベースに関する情報を入力するよう求められます。



7. [次へ] をクリックします。[セットアップ ステータス] 画面が表示されます。

8. インストールが終了すると、[メンテナンスの完了] 画面が表示されます。

9. [はい、今すぐコンピュータを再起動します。] を選択します。

10. [完了] をクリックします。

複雑な分散インストール

複雑な分散シナリオで配置するには

1. 単一のサーバに InterScan MSS をインストールします (80 ページの「集中インストール」を参照)。
2. 追加の InterScan MSS 検索サービス、エンドユーザメール隔離サービス、またはエンドユーザメール隔離データベースをインストールします (92 ページの「検索サービスとエンドユーザメール隔離サービス / データベースの複数インストール」を参照)。

ヒント： MSDE 2000 には次の制限が適用されます。
- データ量 2GB
- 同時ユーザ接続または作業負荷数 5

1 日のメールトラフィックが 30,000 件を上回る場合や、InterScan MSS エンドユーザメール隔離を使用している場合、MSDE を使用しないようにしてください。これは、レポートとログクエリ結果の保存用に十分な空き領域を確保する必要があるためです。

サイレントインストール

サイレントインストールでは、複数の検索サービス、エンドユーザメール隔離サービス、およびエンドユーザメール隔離データベースを同じ設定でインストールすることができます。この場合、各コンピュータでの setup.exe の実行時に、そのつど手動で設定を指定する必要はありません。

サイレントインストールを実行するには、スクリプトにインストール手順を記録し、このスクリプトを実行して追加の InterScan MSS コンポーネントを順次インストールします。同様にアンインストールについても、アンインストール手順を記録したスクリプトを実行することによって、サイレントアンインストールを実行できます。

サイレントインストールには、主に次の 2 つの手順があります。

手順 1 — インストール手順の記録

手順 2 — 追加コンポーネンのインストールスクリプトの実行

インストール手順の記録

インストール手順を記録するには

1. コマンドウィンドウを開き、セットアッププログラムが格納されているフォルダに移動します。

2. utility というサブフォルダに移動します。

3. 指定したスクリプトにインストール手順を記録するために、InstRecord.bat ファイルを実行します。次に例を示します。

   InstRecord.bat scanner.iss

4. setup.exe を入力してインストールプログラムを実行します。80 ページの「集中インストール」を参照してください。

注意： 1. スクリプトの格納先のパスは指定できますが、InstRecord.bat の実行前にすでに存在するパスでなければなりません。
2. スクリプトファイル名には .iss 拡張子が必要です。
3. パスを指定しないと、スクリプトは現在のフォルダに作成されます。

サイレントインストールスクリプトの実行

サイレントインストールスクリプトを使用して追加コンポーネントをインストールするには

1. コマンドウィンドウを開き、セットアッププログラムが格納されているフォルダに移動します。

2. utility というサブフォルダに移動します。

3. InstSilent.bat ファイルを実行すると、事前に作成したサイレントインストールスクリプトを使用してコンポーネントがインストールされます。106 ページの「インストール手順の記録」を参照してください。次に例を示します。

   InstSilent.bat scanner.iss

4. インストールのポップアップページが表示されることなく、バックグラウンドでインストールが実行されます。

注意： インストールが正常に完了したことを確認するには、管理コンソールで [概要] →[システム] タブをクリックして、[管理下のサーバ設定] を確認します。

InterScan MSS 5.18 からのアップグレード

InterScan MSS のインストールプログラムでは、InterScan MSS バージョン 5.18 からのアップグレードが自動的に実行されます。インストールプログラムで InterScan MSS 5.18 が検出されると、次の処理が実行されます。

- 前バージョンの InterScan MSS のアンインストール
- InterScan MSS のインストール
- 既存の設定の移行

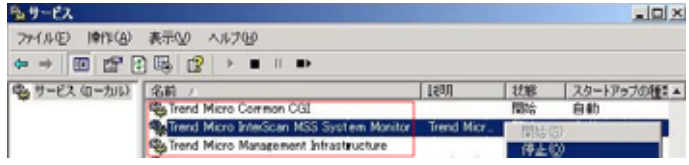
ヒント： 前バージョンの InterScan MSS の設定を移行しない場合は、既存のインストールに InterScan MSS 7.0 をインストールするのではなく、InterScan MSS を完全にアンインストールしてから、インストールを実行することをお勧めします。

アップグレード前のバックアップ

アップグレードで問題が発生した場合、以前の設定にロールバックする必要があります。ロールバック処理をスムーズに実行するために、InterScan MSS 5.18 の可能な限りのデータを保存しておきます。

ヒント： アップグレードを実行する前に、次の手順でデータをバックアップすることをお勧めします。

1. システムサービス管理ウィンドウから、InterScan MSS 5.18 のすべてのサービスを停止します。

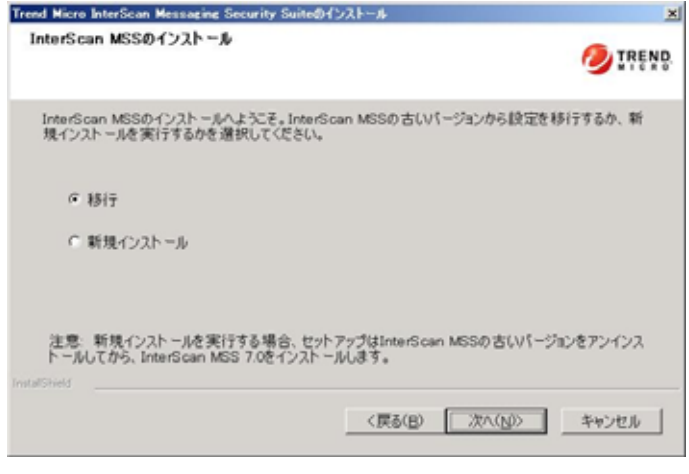


2. システムサービス管理ウィンドウから、IIS のすべてのサービスを停止します。
3. InsterScan MSS 5.18 のインストールフォルダをバックアップします。
4. レジストリからポリシー設定をエクスポートします。
HKEY_LOCAL_MACHINE>SOFTWARE>TrendMicro

移行の実行

移行を実行するには

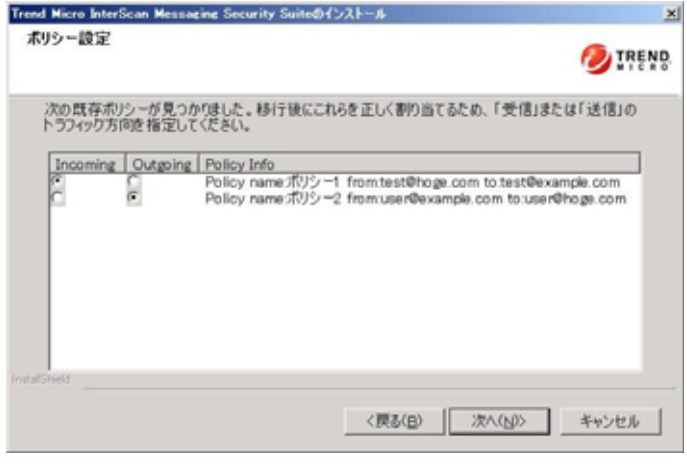
1. [移行] を選択します。



注意 :[新規インストール] を選択すると、InterScan MSS 5.18 がアンインストールされ、InterScan MSS 7.0 がインストールされます。

2. [次へ] をクリックします。[移行情報] ダイアログが表示されます。
注意 : 移行されない前バージョンの設定は、こうした画面で表示されます。これらの設定については、c:¥Imss7InstLog¥Installog¥MigrationReport¥GeneralReport.txt で確認することもできます。

3. [次へ] をクリックします。InterScan MSS 5.18 で特別なルートを指定したポリシーを使用していた場合は、[ポリシー設定] ダイアログが表示されます。

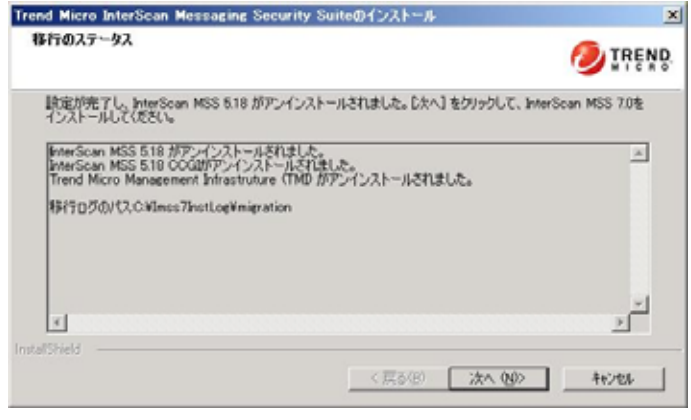


4. [送信] または [受信] ボタンをクリックして、設定するポリシーの方向を選択します。

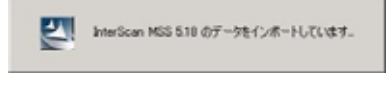
5. [次へ] をクリックします。移行データがバックアップされます。セットアップの確認ダイアログが表示されます。

6. [はい] をクリックします。InterScan MSS 5.18 がアンインストールされます。

[移行のステータス] ダイアログが開き、InterScan MSS 5.18 のアンインストール結果が表示されます。



7. [次へ] をクリックします。InterScan MSS 7.0 を設定し、インストールします (80 ページの「集中インストール」を参照)。最後に、InsterScan MSS 5.18 のデータがインポートされます。



[移行結果] ダイアログが表示されます。

移行されない設定

InterScan MSS 7.0 での変更が多数のため、次の設定は移行されません。

- 隔離領域のパス
- アーカイブフォルダのパス
- 各種ログのパス
- 時間あたりの通知数の制限
- 管理コンソールのパスワード
- シリアル番号
- セキュリティ設定の駆除の試行回数
- セキュリティ設定のウイルスレポート数
- セキュリティ設定の InterScan eManager (以下、eManager) のメッセージサイズ
- ユーザ定義のサブポリシーのウイルスフィルタ
- ウイルスフィルタに設定された、ウイルスが検出されなかった場合のカスタム処理
- ウイルス検索における除外する拡張子の設定

- 詳細コンテンツフィルタに設定された、添付ファイル名またはファイルタイプに一致するキーワードのリスト
- コンテンツフィルタにおけるキーワードの類義語の設定
- オリジナルメッセージのアーカイブに関する設定
- オリジナルメッセージに添付した通知に関する設定
- オリジナルメッセージの添付ファイル転送に関する設定

アップグレード後のロールバック

1. インストールプログラムで、InterScan MSS 7.0 のコンポーネントをすべてアンインストールします。
2. InterScan MSS 5.18 を新規インストールします。
3. システムサービス管理ウィンドウから、実行中の InterScan MSS 5.18 のサービスをすべて停止します。
4. InterScan MSS 5.18 のインストールフォルダを復元します。
5. レジストリから「TrendMicro」を削除します。
6. InterScan MSS 5.18 の以前のポリシー設定をレジストリにインポートします。
7. World Wide Web Publishing Service も含めて、IIS のサービスを開始します。
8. InterScan MSS 5.18 のすべてのサービスを次の順序で開始します。
   - 1) TrendMicro Management Infrastructure サービスの開始
   - 2) TrendMicro Common CGI サービスの開始
   - 3) 他の InterScan MSS 関連サービスの開始

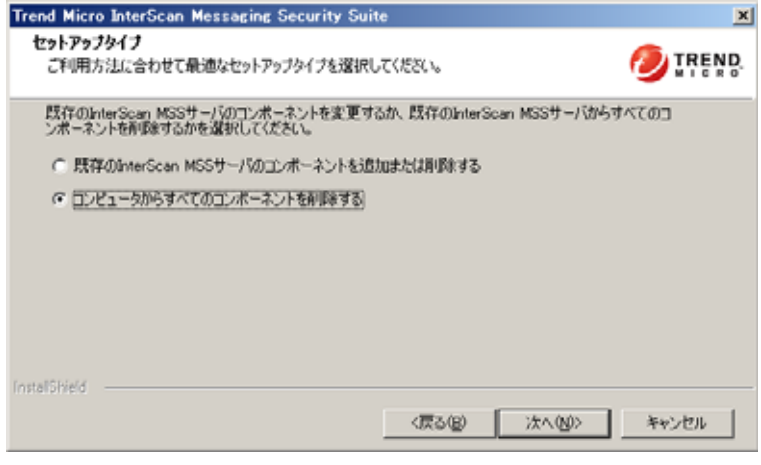
注意： 他の InterScan MSS サービスより先に、TMI と CCGI を開始する必要があります。

アンインストールの実行

この項では、InterScan MSS コンポーネントの削除方法について説明します。セントラルコントローラ、検索サービス、エンドユーザメール隔離の各コンポーネントを、個別に削除することも、まとめて削除することもできます。

InterScan MSS をアンインストールするには

1. Setup.exe をクリックします。[セットアップタイプ] 画面が表示されます。



2. 削除するコンポーネントを選択します。

   すべての InterScan MSS コンポーネントをコンピュータから削除するには

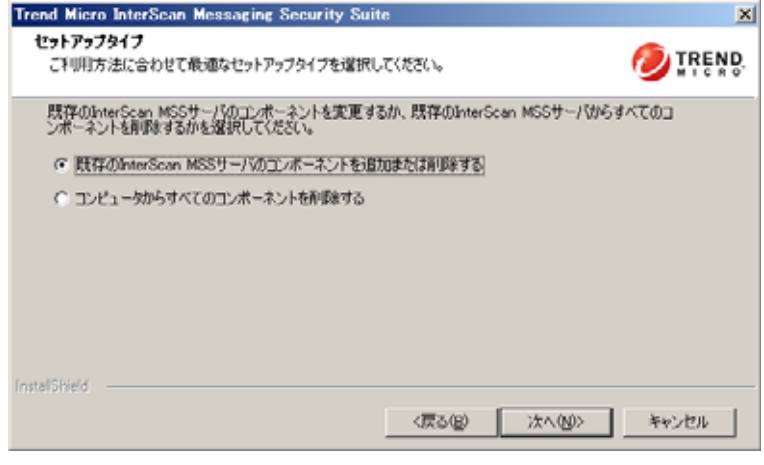
   a. [コンピュータからすべてのコンポーネントを削除する] を選択します。

b. [次へ] をクリックします。確認画面が表示されます。

c. [はい] をクリックして確認します。

選択した InterScan MSS コンポーネントを削除するには

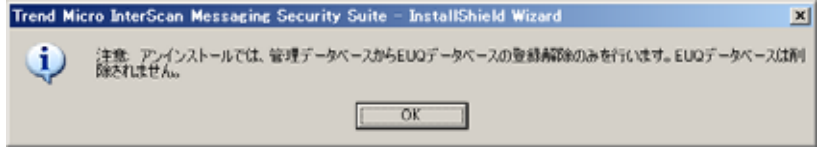
a. 選択したコンポーネントを個別に削除するには、[既存の InterScan MSS サーバのコンポーネントを追加または削除する] を選択します。



b. [次へ] をクリックします。[機能の選択] 画面が表示されます。

c. アンインストールするコンポーネントの選択を解除します。たとえば、エンドユーザメール隔離データベースをアンインストールする場合は、このコンポーネントのオプションのチェックマークをオフにします。

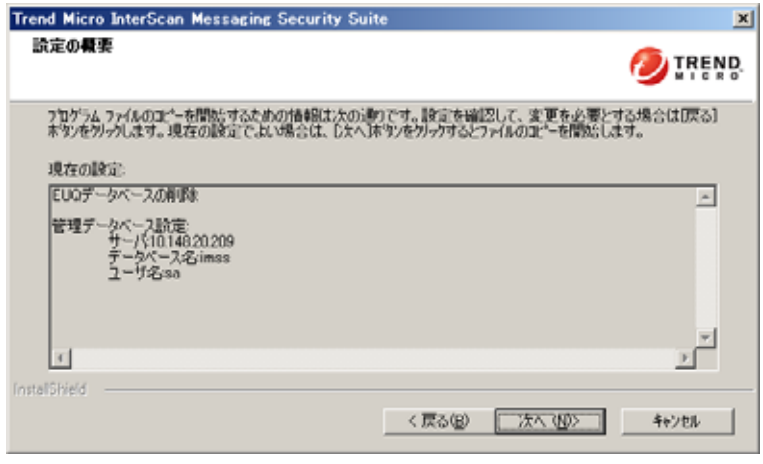
d. [次へ] をクリックします。エンドユーザメール隔離データベースのアンインストールを選択した場合は、次のメッセージが表示されます。



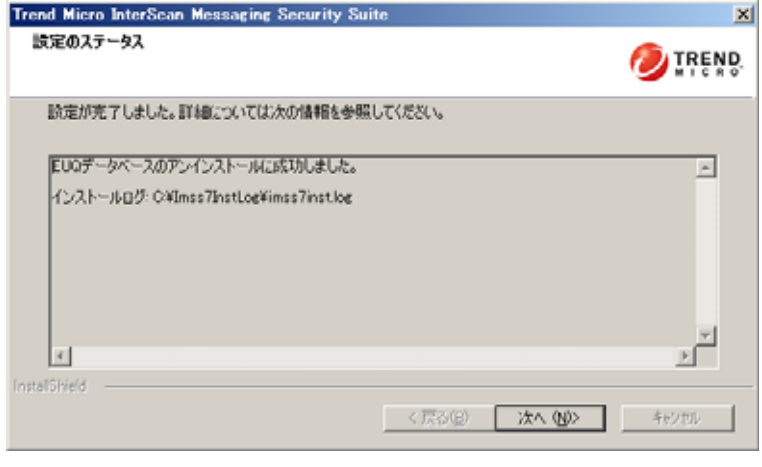
e. [OK] をクリックします。

注意： エンドユーザメール隔離データベースのアンインストールを選択した場合、管理データベースからの隔離データベースの登録解除のみ行われます。他のコンポーネントをすべて削除した後に、手動でエンドユーザメール隔離データベースを削除する必要があります。

3. [次へ] をクリックします。[設定の概要] 画面が表示されます。



4. [次へ] をクリックします。コンポーネントがアンインストールされます。[セットアップステータス] 画面が表示されます。



5. [次へ] をクリックします。[メンテナンスの完了] 画面が表示されます。

6. [完了] をクリックします。

サイレントアンインストール

サイレントアンインストールの手順は、105 ページの「サイレントインストール」で説明している手順と同様です。

注意： サイレントアンインストールは、サイレントインストールスクリプトを記録したコンピュータと同様の環境のコンピュータで実行してください。
サイレントインストールスクリプトの記録時やサイレントインストールの実行時には、サービス管理画面をすべて閉じてください。

MSDE から SQL Server 2005 Express へのアップグレード

InterScan MSS 管理データベースとエンドユーザメール隔離データベースは、Microsoft SQL Server Desktop Engine (MSDE) を使用してインストールできます。ただし、Microsoft の標準のライフサイクルポリシーに従い、MSDE のメインストリームサポートは 2008 年 4 月 8 日に終了します。この項では、InterScan MSS 7.0 を MSDE の新バージョンである SQL Server 2005 Express と統合する方法について説明します。

SQL Server 2005 Express のインストールの前提条件

SQL Server 2005 Express をインストールする前に、次のものをダウンロードしてインストールしておく必要があります。

- Windows Installer 3.1
- .NET Framework 2.0

詳細については、次の Web ページを参照してください。

https://www.microsoft.com/japan/technet/prodtechnol/sql/2005/sqlupgrd.mspx

インストールされた MSDE から SQL Server 2005 Express へのアップグレード

InterScan MSS 7.0 で MSDE がインストールされている場合は、次の手順で MSDE を SQL Server 2005 Express に完全にアップグレードできます。

手順 1 — すべての InterScan MSS サービスの停止

手順 2 — InterScan MSS データベースのバックアップの作成

手順 3 — SQL Server 2005 Express のインストール

手順 4 — データベース管理者のパスワードのリセット

手順 5 — InterScan MSS サービスの開始

手順 1 — すべての InterScan MSS サービスの停止

InterScan MSS サービスを停止するには

1. InterScan MSS 7.0 コンポーネントがインストールされているコンピュータで管理者としてログオンします。
2. コマンドプロンプトを開き、次のコマンドを入力して InterScan MSS サービスを停止します。

```
net stop TmImssManager
net stop TmImssAdminUI
net stop TmImssTasks
net stop TmImssScan
net stop TmImssMTA
net stop TmImssPolicy
net stop TmImssIpprofiler
net stop TmImssCMAgent
net stop TmImssEuqUI
```

手順 2 — InterScan MSS データベースのバックアップの作成

MSDE のアップグレードを実行する前に、InterScan MSS 管理データベースとエンドユーザメール隔離データベースのバックアップを作成することをお勧めします。それにより、アップグレード中に予期しない事態が発生しても、restore database コマンドを使用してデータベースを元の状態にロールバックすることができます。

InterScan MSS データベースのバックアップを作成するには

1. コマンドプロンプトを開き、コマンド osql を入力して、アップグレード対象のインスタンスに接続します。

   Windows 認証を使用してローカルの初期設定の MSDE インスタンスに接続するには、コマンド osql -E を入力します。

2. osql コマンドプロンプトで次のコマンドを入力して、MSDE インスタンス上の InterScan MSS データベースのバックアップを作成します。

```
1> backup database imss to disk='c:¥imss.dat'
2> GO
1> backup database imsseuq to disk='c:¥imsseuq.dat'
2> GO
```

手順 3 ― SQL Server 2005 Express のインストール

SQL Server 2005 Express をインストールするには

1. MSDE がインストールされているコンピュータで管理者としてログオンします。

2. sqlexpr.exe を入力して、SQL Server 2005 Express のセットアッププログラムを開始します。

   詳細については、次の Web ページを参照してください。
   https://www.microsoft.com/japan/technet/prodtechnol/sql/2005/sqlupgrd.mspx

注意： 1. MSDE アップグレードの登録情報画面で、詳細構成オプションを使用することをお勧めします。
2. [インスタンス名] 画面で InterScan MSS が使用するインスタンスを選択します。
3. MSDE から SQL Server 2005 Express へのデータベースのアップグレード時には、[Windows 認証モード] を選択します。

手順 4 — データベース管理者のパスワードのリセット

Windows 認証モードでは、MSDE から SQL Server 2005 Express へのアップグレード時にパスワードは不要です。ただし、アップグレード後に既存の InterScan MSS データベースに接続するためには、データベース管理者のパスワードをリセットする必要があります。

データベース管理者のパスワードをリセットするには

1. コマンドプロンプトを開きます。
2. sqlcmd -E を入力して sqlcmd セッションを開始します。
3. 次のコマンドを入力して、sa アカウントを有効にし、sa のパスワードを設定します。

```
1> ALTER LOGIN sa ENABLE
2> GO
1> ALTER LOGIN sa WITH PASSWORD = '<password>'
2> GO
```

注意： 以前の MSDE sa パスワードを使用する必要があります。

手順 5 — InterScan MSS サービスの開始

InterScan MSS サービスを開始するには

1. InterScan MSS のサービスがインストールされているコンピュータで管理者としてログオンします。
2. コマンドプロンプトで次のコマンドシーケンスを入力します。

```
net start TmImssManager
net start TmImssAdminUI
net start TmImssTasks
net start TmImssMTA
net start TmImssScan
net start TmImssPolicy
net start TmImssIpprofiler
net start TmImssCMAgent
net start TmImssEuqUI
```

新規インストール時の SQL Server 2005 Express との統合

InterScan MSS 7.0 の新規インストールを実行する場合は、次の手順で SQL Server 2005 Express と InterScan MSS 7.0 を統合できます。

手順 1 — SQL Server 2005 Express のインストール

手順 2 — ネットワークアクセスの有効化

手順 3 — SQL Server Browser サービスのスタートアップの自動化

手順 4 — InterScan MSS 7.0 のインストール

手順 1 — SQL Server 2005 Express のインストール

SQL Server 2005 Express をインストールするには

1. 管理者としてログオンします。
2. sqlexpr.exe を入力して、SQL Server 2005 Express のセットアッププログラムを開始します。

   詳細については、次の Web ページを参照してください。
   https://www.microsoft.com/japan/technet/prodtechnol/sql/2005/sqlupgrd.mspx

注意： SQL Server 2005 Express の新規インストールの実行時に [混合モード] (Windows 認証と SQL Server 認証) を選択します。

手順 2 — ネットワークアクセスの有効化

初期設定では、SQL Server 2005 Express のインストールにより、指定されたパイプと TCP/IP プロトコルは無効になります。これらのプロトコルは、SQL Server 構成マネージャを使用して有効にできます。

詳細については、次の Web ページを参照してください。
https://www.microsoft.com/japan/technet/prodtechnol/sql/2005/sqlupgrd.mspx

手順 3 — SQL Server Browser サービスのスタートアップの自動化

SQL Server Browser サービスは、SQL Server 2005 Express のインスタンスが待機するネットワークポートを識別します。SQL Server 2005 セキュリティ構成ユーティリティを使用して、SQL Server Browser サービスのスタートアップの種類を自動に設定します。

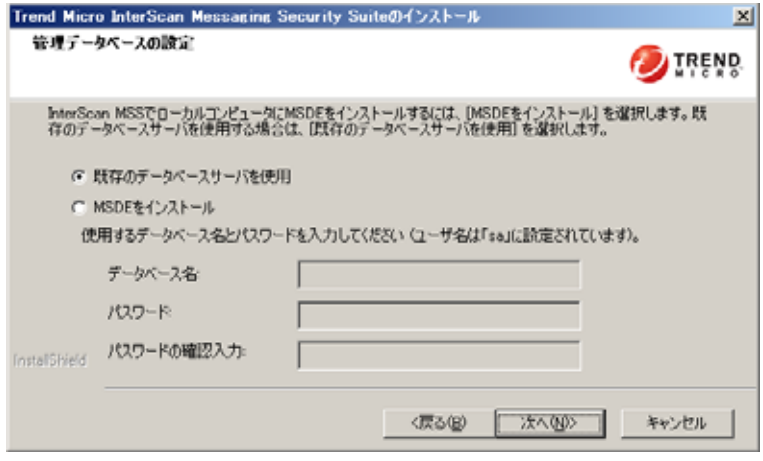
詳細については、次の Web ページを参照してください。
https://www.microsoft.com/japan/technet/prodtechnol/sql/2005/sqlupgrd.mspx

手順 4 — InterScan MSS 7.0 のインストール

InterScan MSS 7.0 のインストール方法の詳細については、80 ページの「集中インストール」を参照してください。

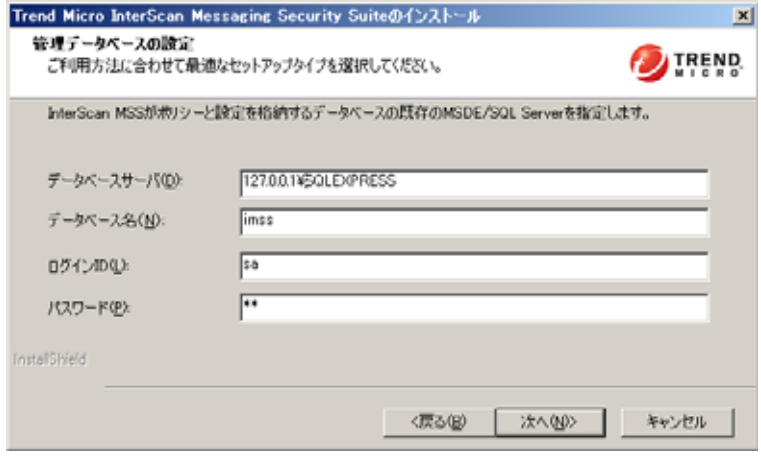
インストール時に InterScan MSS 7.0 を SQL Server 2005 Express と統合する際には、次の点に注意してください。

1. [管理データベースの設定] 画面で [既存のデータベースサーバを使用] を選択します。



2. [次へ] をクリックします。

3. 管理データベースの設定情報を入力します。[データベースサーバ] フィールドで、データベースインスタンス名を必ず付加します。SQL Server 2005 の初期設定のインスタンス名は SQLEXPRESS です。



第 5 章

トラブルシューティングとサポート情報

この章では、Trend Micro InterScan Messaging Security Suite (以下、InterScan MSS) の一般的な問題のトラブルシューティング、トレンドマイクロ製品 Q&A の検索、およびトレンドマイクロサポートへの問い合わせについて説明します。

この章の内容は次のとおりです。

- 128 ページの「トラブルシューティング」
- 129 ページの「よくある質問 (Q&A)」
- 136 ページの「製品サポート情報」
- 136 ページの「サポートサービスについて」
- 137 ページの「製品 Q&A のご案内」
- 137 ページの「セキュリティ情報」
- 139 ページの「ウイルス解析サポートセンター「TrendLabs」」

トラブルシューティング

表 5-1 は、InterScan MSS のインストール時に発生する可能性がある一般的な問題を示しています。この表で、それぞれの問題の解決策を参照してください。その他の問題については、トレンドマイクロの製品 Q&A を確認してください。

InterScan MSS の管理または保守に関連する問題のトラブルシューティングとよくある質問については、InterScan MSS の管理者ガイドを参照してください。

問題	推奨される解決策
NRS のインストール時、NRS アクティベーションコードが認証されない	アクティベーションコードを認証するために、NRS インストールスクリプトはインターネットでトレンドマイクロにアクセスします。 DNS サーバが正しく動作していることと、NRS をインストールするコンピュータからインターネットにアクセスできることを確認してください。
データベースアクセスの問題が原因で InterScan MSS が正常に動作しない (InterScan MSS が Windows 2000 SP4 にインストールされている場合)	MDAC のバージョンが 2.8 SP1 より下です。 次の Microsoft Web サイトから最新バージョンの Microsoft MDAC をダウンロードして、インストールしてください。 http://www.microsoft.com/downloads/details.aspx?FamilyID=78cac895-efc2-4f8e-a9e0-3a1afbd5922e&DisplayLang=ja

表 5-1. 問題のトラブルシューティング

よくある質問 (Q&A)

インストール

InterScan 管理データベースは単独でインストールできますか。

できます。InterScan MSS 管理データベースは、次の 2 つの方法により単独でインストールできます。

- インストールプログラムを実行し、InterScan MSS の他のコンポーネントは選択しないで、InterScan MSS データベースのみを設定します。
- ターゲットコンピュータに既存のデータベースサーバが存在する場合は、コマンドインタフェースでインストールプログラムを実行します。
  - セットアップフォルダに移動します。
  - 次のコマンドを使用して、インストールプログラムを実行します。

    setup.exe /zOnlyInstDB
  - インストール画面の指示に従って、InterScan MSS 管理データベースをインストールします。

注意： InterScan MSS 管理データベースのインストールを完了したら、インストールプログラムを実行して他のコンポーネントをインストールします。この場合、「sa」以外のアカウントを使用して InterScan MSS データベースに接続します。

ターゲットコンピュータに複数のデータベースインスタンスをインストールできますか。

できません。ターゲットコンピュータに既存のデータベースが存在する場合は、そのデータベースのみを InterScan MSS データベースまたはエンドユーザメール隔離データベースとして使用します。または、既存のデータベースをアンインストールし、新しい MSDE データベースをインストールします。MSDE は InterScan MSS インストールパッケージに含まれています。

インストールできる検索サービスの数はいくつですか。

検索サービスはいくつでもインストールできます。

インストールできるエンドユーザメール隔離サービスおよびエンドユーザメール隔離データベースの数はいくつですか。

エンドユーザメール隔離サービスとエンドユーザメール隔離データベースは 8 つまでインストールできます。

エンドユーザメール隔離サービスごとに、エンドユーザメール隔離データベースを個別にインストールする必要がありますか。

その必要はありません。エンドユーザメール隔離サービスには少なくとも 1 つのエンドユーザメール隔離データベースが必要ですが、複数のエンドユーザメール隔離サービスで 1 つのエンドユーザメール隔離データベースを共有することができます。

アンインストール時に InterScan MSS データベースは削除されますか。

削除されません。アンインストール時には、管理データベースからのエンドユーザメール隔離データベースの登録解除のみ行われます。InterScan MSS エンドユーザメール隔離データベースは、管理コンソールから再登録することができます。

インストール時に以前の InterScan MSS データベースは削除できますか。

できません。これは、インストールプログラムが InterScan MSS データベースを削除しようとするときに、アプリケーションがデータベースに接続しているためです。以前のデータベースへの接続をすべて削除した後、データベースを削除し、新しいデータベースを作成してください。

InterScan MSS 7.0 は初期設定のパスにインストールする必要がありますか。

その必要はありません。任意のパスを指定できます。ただし、64 ビットの OS の場合、X:¥Program Files (X はシステムディスク) にはインストールできません。このフォルダは 64 ビットプログラム用に予約されています。

ターゲットコンピュータで管理コンソールへのショートカットが機能しないのはなぜですか。

ターゲットコンピュータが Windows 2003 プラットフォームで動作している場合、ショートカットのアドレスをブラウザの信頼済みゾーンに追加します。

データベースプロセスの状態に応じて、次のことを実行します。

- データベースプロセスが動作していない場合 — データベースサービスを開始して、管理コンソールサービスを再起動します。
- データベースプロセスが動作している場合 — データベースの起動前に管理コンソールを起動した場合は、管理コンソールサービスを再起動します。

InterScan MSS はドメインアカウントを使用してデータベースにアクセスできますか。

できません。InterScan MSS 7.0 は Windows 認証には対応していません。

データベースサーバをホスト名で参照できますか。

できます。「<IP アドレス >¥< インスタンス >」または「< ホスト名 >¥< インスタンス >」として指定できます。

サーバの IP アドレスは変更できますか。

できます。

サーバの IP アドレスを変更するには

a. すべての InterScan MSS サービスを停止します。

b. サーバの IP アドレスを変更します。

c. コントロールパネルで ODBC DSN の IP アドレスを変更します。

d. InterScan MSS 設定フォルダ内の ODBC.ini と EUQ.ini で、IP アドレスを変更します。

e. 次のファイルで、データベースの URL を変更します。

%IMSS_HOME%¥ui¥adminUI¥webapps¥ROOT¥WEB-INF¥struts-config-common.xml

f. 次のデータベースデータを変更します。

- Tb_component_list — コンピュータ名とすべての検索サービスの IP アドレスを指定します。
- Tb_euq_db_info — エンドユーザメール隔離データベースのコンピュータ設定を指定します。
- Tb_global_setting — セクション [cmagent] の名前 [ConfigUrl] で、管理コンソールの URL を変更します。

g. MTA フローに合わせて tsmtpd.ini を変更します。

h. すべての InterScan MSS サービスを再開します。

SNMP 通知機能の MIB ファイルはどこにありますか。

このファイルは %IMSS_HOME%¥help¥IMSS70_win.mib にあります。

InterScan MSS 5.18 の 2 バイト文字を移行するにはどうしたらいいですか。

移行前に、言語設定に誤りがないことを確認してください。

a. 東アジア言語のファイルをインストールします。Windows 2003 の場合、[コントロール パネル]→[地域と言語のオプション]→[言語] の順に選択し、東アジア言語のインストールファイルを選択します。

b. InterScan MSS 5.18 で使用していた 2 バイト文字言語に合わせて、非 Unicode プログラムの言語設定を中国語 / 日本語に変更します。

c. 移行インストールを実行します。

アップグレード

移行時に InterScan MSS 5.18 の設定はすべて維持されますか。

維持されません。InterScan MSS 7.0 ではアーキテクチャが変更されたため、一部、維持できない設定があります。これらの設定については、移行時に InterScan MSS 7.0 のインストールプログラムによって新しい値を指定するように指示されます。また、これらの設定は次の一般移行レポートで検出することもできます。

C:¥Imss7InstLog¥migration¥installlog¥MigrationReport¥GeneralReport.txt

InterScan MSS 5.18 のポリシーと InterScan MSS 7.0 のルールとのマッピングの関係はどのようになりますか。

マッピングの関係については、次の詳細移行レポートで示されます。

C:¥Imss7InstLog¥migration¥installlog¥MigrationReport¥DetailReport.txt

InterScan MSS 5.18 の複数の検索サービスを移行するにはどうしたらいいですか。

InterScan MSS 5.18 の複数の検索サービスを移行するには

a. 移行に最も適した設定を使用している検索サービスから移行を実行します。

b. 残りの検索サービスをアンインストールします。

c. 複数の検索サービスを追加します。

移行後に InterScan MSS 5.18 にスムーズにロールバックできますか。

できます。ロールバック手順の詳細については、113 ページの「アップグレード後のロールバック」を参照してください。

エンドユーザメール隔離コンポーネントのみがインストールされたコンピュータ上で移行を実行できますか。

できません。InterScan MSS 5.18 検索サービスがインストールされたコンピュータから移行を実行してください。

移行後にスパムメール対策ルールを簡素化するにはどうしたらいいですか。

InterScan MSS 5.18 のすべてのポリシーのスパムメール対策フィルタ設定を維持するために、1 つのスパムメール対策フィルタを InterScan MSS 7.0 内の 1 つのスパムメール対策ルールに移行します。移行後にスパムメール対策ルールの数を減らす場合は、次を実行します。

a. 移行後に新しいスパムメール対策ルールを作成します。

b. 移行したスパムメール対策ルールをすべて削除します。

移行時には、どのデータが内部アドレスのソースになりますか。

InterScan MSS 7.0 で InterScan MSS 5.18 の内部ドメインを維持するために、次のフィールドからすべてのドメインが抽出されます。

- 受信ポリシールートの「To」フィールドのドメイン
- 送信ポリシールートの「From」フィールドのドメイン

注意： 上記の 2 つのフィールドにアドレスグループが設定されている場合、アドレスグループ内のすべてのドメインが抽出されます。

移行時にフィルタとポリシーはどのようにマッピングされますか。

InterScan MSS 5.18 と InterScan MSS 7.0 のアーキテクチャは非常に異なっています。そのため、移行モジュールにより、InterScan MSS 5.18 のすべてのフィルタが InterScan MSS 7.0 の関連するルールに次のようにマッピングされます。

a. ウイルスフィルタ — 移行後は、InterScan MSS 5.18 で使用していたウイルスフィルタの数にかかわらず、送信 / 受信の両方で 1 つのウイルスルールのみにマッピングされます。

   - InterScan MSS 5.18 でウイルスフィルタが 1 つでも「アクティブ」になっていると、ウイルスルールの状態は「有効」になります。
   - それ以外の場合は、移行後のウイルスルールの状態は「無効」になります。

b. フィルタ — 移行モジュールにより、移行後は 1 つのスパムメール対策フィルタが 1 つのスパムメール対策ルールにマッピングされます。

c. eManager フィルタ

   - InterScan MSS 5.18 で eManager フィルタが SMTP と POP3 の両方のトラフィックに対して「有効」に設定されている場合、移行後はその eManager フィルタ 1 つに対して 2 つのルールが作成されます。

- InterScan MSS 5.18 で eManager フィルタが SMTP と POP3 の両方のトラフィックに対して「無効」に設定されている場合、移行後はその eManager フィルタ 1 つに対してルールが 1 つのみ作成されます。ルールの方向は「受信と送信の両方」です。必要に応じて、InterScan MSS 7.0 で POP3 方向に関連するルールを追加できます。

製品サポート情報

InterScan MSS のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「スタンダードサポート サービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話、FAX、メールなどをご利用ください。サポートセンターの連絡先は、「スタンダードサポート サービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意： サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

製品 Q&A のご案内

トレンドマイクロの Web サイトでは、製品 Q&A の情報を提供しています。これは、トレンドマイクロの製品に関する技術的な質問と、それに対する回答を集めたものです。製品 Q&A には、次の URL からアクセスできます。

中小 / 中堅企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/smb/search.do

大企業のお客さま

http://esupport.trendmicro.co.jp/supportjp/enterprise/search.do

製品 Q&A では、お使いの製品名およびキーワードを指定して、知りたい情報を検索できます。たとえば製品のマニュアル、ヘルプ、Readme ファイルなどに記載されていない情報が必要な場合に、製品 Q&A を利用してください。

トレンドマイクロでは製品 Q&A の内容を常に更新し、新しい情報を追加しています。

セキュリティ情報

セキュリティ情報の入手先

トレンドマイクロでは、最新のセキュリティ情報をインターネットで公開しています。トレンドマイクロのセキュリティ情報 Web サイトでは、ウイルスやインターネットセキュリティに関する最新の情報を入手できます。セキュリティ情報 Web サイトは、次の URL からアクセスできます。

http://www.trendmicro.co.jp/vinfo/

管理コンソールからセキュリティ情報サイトにアクセスすることもできます。セキュリティ情報サイトにアクセスするには、管理コンソールの画面の右上にあるリストボックスから[セキュリティ情報] リンクを選択します。

セキュリティ情報 Web サイトでは、次の情報を閲覧できます。

- ウイルス名やキーワードから検索できるウイルスデータベース
- コンピュータウイルスの最新動向に関するニュース
- 現在流行中のウイルスや不正プログラムの情報
- デマウイルスまたは誤警告に関する情報
- ウイルスやネットワークセキュリティの予備知識

セキュリティ情報 Web サイトに定期的にアクセスして、流行中のウイルス情報などを入手することをお勧めします。メールによる定期的なウイルス情報配信を希望する場合は、警告メール配信の登録フォームを利用してメールアドレスを登録してください。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出 / 駆除できない場合などに、感染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロのウイルスデータベース検索サイトにアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

http://www.trendmicro.co.jp/vinfo/virusencyclo/default.asp

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

http://inet.trendmicro.co.jp/esolution/attach_agreement.asp

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

ウイルス解析サポートセンター「TrendLabs」

トレンドマイクロのウイルス解析サポートセンター「TrendLabs」(トレンドラボ) は、フィリピンセンターを本部として、米国、日本、台湾、ドイツ、アイルランド、中国の各国センターで構成されています。24 時間体制でウイルスの活動を監視するウイルス解析エンジニアを含む 800 名以上 (2006 年 1 月現在) のスタッフが、セキュリティに関する最新の情報を収集し、高品質なサービスとソリューションを迅速かつ効果的に世界各国のトレンドマイクロのパートナーとお客さまに提供しています。

「TrendLabs」では、品質保証の ISO9001:2000 認定 (フィリピン)、国際規格 COPC-2000 規格 (フィリピン)、英国の国家規格 ITIL: BS15000 (ドイツ)、情報セキュリティマネージメントの英国規格 BS7799 (フィリピン) を取得しています。

索引

英数字

Apache 50
  Tomcat 49
CCGI 113
Control Manager
  概要、Control Manager
    概要 25
Control Manager エージェント、エージェント
  Control Manager 25
CPU の要件 32
Firefox 33
IMSSMGR 49
Internet Explorer 33
InterScan MSS 14
InterScan MSS コンポーネント
  インストール 49
  エンドユーザメール隔離データベース 41
  エンドユーザメール隔離プライマリおよびセ
  カンダリサービス 38
  管理データベース 35
  検索サービス 36
  セントラルコントローラ 35
  ポリシーサービス 37
  ポリシーサービスの同期 37
InterScan MSS について 14
IP フィルタ
  概要 41
IP プロファイラ 15
  概要 41
  機能 43
MTA 機能、便宜的な TLS 15
Named Server 49
NRS 15
  概要 42
  機能 43
  サービス 42
Readme ファイル 10
TMI 113
Tomcat 49、50
TrendLabs 139
Web エンドユーザメール隔離 15
x64 85

あ

アーカイブ 15
アーカイブおよび隔離領域の一元化 15
インストール 31
  IP フィルタ、インストール
    エンドユーザメール隔離 75
  SMTP ゲートウェイ 59
  クラスタ化 69
  シナリオ 61
  集中 80
  ファイアウォールなし 55、56、57、59
  ファイアウォールの内側 57
  ファイアウォールの外側 56
  複数の検索サービスとエンドユーザメール隔

離サービス / データベース 92
エンドユーザメール隔離 15
オンラインヘルプ 10

か

隔離 15
管理データベース 49
検索サービス 38
コンポーネントおよびサブモジュールのインストール 49
コンポーネントの追加 93

さ

最小要件 32
サイレントインストール 105
システム要件 32
新機能 14
スパイウェアとグレーウェア 24
スパムメール対策 15
スワップ領域の要件 33
設定ウィザード 15
セントラルコントローラ 37

た

対象読者 11
ディスク領域の要件 32
データベース
セントラルコントローラ 35
データベースサーバ 49
テクニカルサポート 136
ドキュメント 10
トラブルシューティング 128
NRS 128

は

はじめに 9
パターンマッチング 16
フィルタ、機能 20
フェイルオーバー 76
ブラウザ要件 33
ポリシー 14
ポリシーサービス 37
ポリシーの一元化 14

ま

マスメーリング型ウイルス
パターン 19
メール脅威
スパムメール 18
非生産的メッセージ 18
メモリの要件 32

や

要件 32

ら

レポート 14
ロールバック 113
ログ 14
ログ機能の一元化 14